

Pour la Science



POUR LA

SCIENCE

Juin 1999

édition française de

SCIENTIFIC
AMERICAN

Dossier :
*La sécurité
sur l'Internet*

Janard

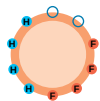
Les raz-de-marée



BLOC-NOTES

de Didier Nédon

5



JEU-CONCOURS

Dîner de mathématiciens

par Pierre Taugne

6

TRIBUNE DES LECTEURS

7



POINT DE VUE

La déformation par la recherche

par Bernard Beauzamy

8



PRÉSENCE DE L'HISTOIRE

Les découvertes oubliées d'Alan Turing

par Jack Copeland et Diana Proudfoot

12



SCIENCE ET CHIMIE

Arômes et réactions

par Hervé Tots

16



PERSPECTIVE

■ L'astronomie astrologue ■ L'amour est aveugle

■ Un très vil atelier ■ Turbulence et transition

de phase ■ Les papillonsavirus ■ Une «perle de soufre»

■ Cartes d'extinction ■ Calcul verbal

20



IDÉES DE PHYSIQUE

Le gravitryne

par André Delhoucq

100



LOGIQUE ET MATHÉMATIQUES

Premiers jumeaux frères ennemis?

par Jean-Paul Delahaye

102



Tours, tortillements, topologie et téléphone

par Ian Stewart

108



ANALYSES DE LIVRES

110

Les Orchidées de France, Belgique et Luxembourg, ouvrage collectif de la Société française d'Orchidophilie

sous la direction de Marcel Bourméras

■ Œuvres de Pierre de Fermat (I. La théorie des nombres), textes traduits par Paul Tannery, introduits et commentés par R. Rashed, Ch. Houzel et G. Christol

■ Maths et Maple, de Jean-Michel Ferrard

■ The Practice of Medicinal Chemistry, sous la direction de Camille Wermuth

Les 500 paires de lunettes Éclipse 99 que nous avons réservées à nos lecteurs sont maintenant épuisées. Vous pouvez vous en procurer dans notre boutique ou auprès de la Société astronomique de France (voir sur notre site Web).

Dossier

La sécurité sur l'Internet

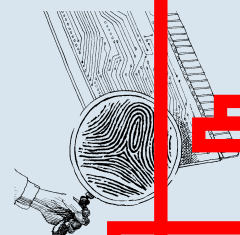
29

Pirates sur l'Internet

30

par Carolyn Meinel

Les pirates informatiques emploient un arsenal varié pour commettre leurs méfaits. Pourtant, aucun d'eux n'est invincible.

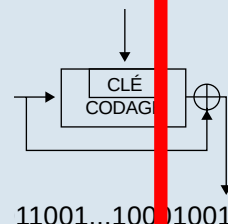


Cryptographie et réseau

38

par Philip Zimmermann

Des systèmes de cryptographie assurent le secret des transmissions électroniques. De nouveaux systèmes encore plus sûrs sont à l'étude.

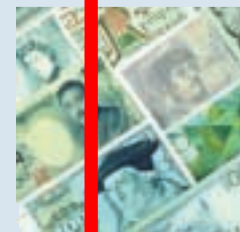


Le paiement sur l'Internet

45

par Octavien Ureche et Réjean Lamondon

L'essor du commerce électronique nécessite de nouveaux moyens de paiement numériques, adaptés au monde virtuel de l'Internet.



Pour la libéralisation de la cryptographie

50

par Ronald Rivest

L'un des pionniers de la sécurité informatique s'oppose au contrôle gouvernemental de la cryptographie.



Les galets, outils du Paléolithique

52

par Sophie A. de Beaune

Des galets non taillés révèlent l'invention de gestes techniques avant la fabrication d'outils spécialisés.



Les cellules souches embryonnaires

58

par Roger Tsien

Récemment isolées, ces cellules semblent capables d'engendrer la quasi-totalité des types de cellules de l'organisme.



Les tsunamis

64

par Frank González

On ne peut lutter contre des vagues hautes comme des immeubles de dix étages et rapides comme un cyclomoteur. En revanche, on évite des dégâts si l'on sait prévoir leur arrivée sur les côtes.

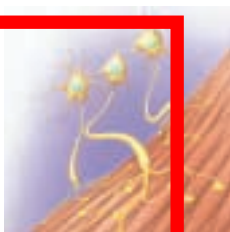


Le syndrome postpolio

76

par Lauro Holte

Plusieurs décennies après avoir retrouvé leur force musculaire, les personnes qui ont eu la poliomyélite se sentent souvent fatiguées et ressentent des douleurs.



Les kangourous carnivores

82

par Stephen Wroe

À l'opposé des kangourous et des koalas actuels, certains marsupiaux australiens ont été de redoutables prédateurs.

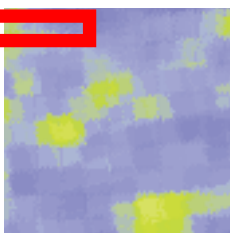


Le ciel infrarouge vu de l'espace

88

par A. Abernethy, F. Boulanger, G. Lagache, L. Barlow et J.-L. Puget

Le satellite ISO a déterminé la nature des poussières du milieu interstellaire et mesuré le rythme de formation des étoiles au cours de l'évolution de l'Univers.



ÉDITORIAL

La grand'peur de l'Internet

Trisson in :

Il pratique l'Internet, Madame, aussi bien qu'un hacker.

Philanthropiste :

L'Internet, l'Internet, ah quel plaisir ma sœur!

Ah permettez, de grâce,

Que pour l'amour du Net, Monsieur, on vous embrasse!

Ainsi aurait pu ironiser Molière, dont nous savons consulter les œuvres sur l'Internet, lire des commentaires sur la vie de l'auteur... tout cela gratuitement. Bel et bon. Nous pouvons aussi commander les œuvres de l'écrivain en laissant notre numéro de carte bleue.

Là, le bât blesse. Un numéro de carte peut être copié par un pirate qui aurait le loisir, cela s'est vu, de commander à votre place et à son profit. Les messages sur l'Internet sont-ils vulnérables? Comment les sécuriser?

En les chiffrant. Mais ce chiffrement est-il inviolable? Le dossier que nous présentons, *La sécurité sur l'Internet (pages 29 à 51)*, détaille le «combat douteux» entre l'épée des méthodes de piratage et le bouclier des logiciels de protection. Combat douteux, car la mise à disposition de ces logiciels n'inspire-t-il pas les pirates qui apprendront à les contourner? Inversement, la connaissance des moyens de piratage autorise des moyens de cryptographie plus sûrs. Heureusement les pirates sont plus malicieux que malveillants et les méthodes qu'ils utilisent pour violer le secret ne sont pas secrètes : un congrès mondial de pirates se réunit à Las Vegas chaque été...

Autre antagonisme : dans son article sur les premiers jumeaux (*page 102*), Jean-Paul Delahaye expose les recherches de Thomas Nicely et explique comment ce chercheur a détecté un grave défaut du *Pentium*. Seul un universitaire libre des contraintes de temps pouvait mener à bien cette enquête. À l'inverse, Bernard Beauzamy critique l'efficacité des titulaires d'un doctorat (*La déformation par la recherche, page 8*), lesquels n'auraient pas, d'après les industriels qui les emploient, les soucis nécessaires de rentabilité.

La critique de la formation des doctorants fait mal, mais il n'est pas de raison supérieure qui justifierait de taire ces opinions.

Philippe BOULANGER

Par Didier Nordon

Tension sur le porc

Étant donné un problème, il y a autant de réponses que de professions qui prétendent avoir des lumières dessus. Exemple. Les lignes à haute tension ont-elles un effet néfaste sur le bétail parqué à proximité ? À cette question, chaque profession répond suivant son idiosyncrasie. Les paysans disent oui et se plaignent ; EDF hausse les épaules et répond non, bien sûr ; les chercheurs scientifiques hésitent et sont divisés ; enfin, les porcs deviennent cannibales (*Le Monde*, 30 mars 1999).

C'est évidemment la réponse des porcs qui est la plus intéressante. Les lignes à haute tension les rendraient cannibales. Est-ce à dire qu'ils dégustent les hommes qui s'approchent d'eux ? Non. Consultons le dictionnaire : un « animal cannibale » est un animal qui dévore ceux de son espèce ; cette expression est calquée sur celle de « sauvage cannibale ». Quant à ces voyageurs blancs qui craignaient d'être mangés par les indigènes, il avaient rien de racistes. L'adjectif « cannibales » désigne ceux qui dévorent leur propre espèce ; avoir peur d'être avalé par les sauvages cannibales, c'est donc reconnaître qu'on est de

la même espèce qu'eux. Merveilleuse preuve d'arrogance !

Mais tout cela ne nous dit pas si la tendance des porcs au cannibalisme est effectivement accrue lorsqu'ils sont à proximité de lignes à haute tension. Nous n'avons pas perdu notre temps, cependant, puisque, à méditer sur les porcs, nous avons approfondi notre connaissance de l'âme humaine.

Obsession textuelle

Avez-vous lu le roman de Sainte-Beuve intitulé *Volupté* ? En ce qui me concerne, la réponse est « non », ce qui prouve que j'étais bien en classe. Le professeur qui nous en a parlé, en effet, nous avait avertis que si, attirés par ce titre prometteur, nous espérions trouver des détails croquillants, nous serions fort déçus.

Le temps a passé, mon tour est venu d'éduquer la jeunesse. Voici donc, si elle lui est utile, l'histoire d'un roman qui n'est

Diamond intitulé *Pourquoi l'amour est un plaisir*, sous-titre « L'évolution de la sexualité humaine », et orné en couverture de photos torrides représentant de passionnés baisers hollywoodiens. Néanmoins, attendre un contenu en rapport serait une

erreur. Naturaliste austère, l'auteur explique comment fonctionne la polygynie chez le gobe-mouche noir ; disserte sur la dihydrotestostérone ; compare, du point de vue de l'abondance de la descendance, la polygamie des femmes Tre-ba du Tibet et celle d'oiseaux (les phalaropes femelles)... Enfin, il ramène le mythe de Don Juan à de justes proportions : Don Juan est un mirable, comparé au gobe-mouche. Séduire mille et trois Espagnoles n'est pas impressionnant. « Si les conquêtes de Don Juan se sont étalées sur trente ans, il n'a séduit qu'une Espagnole tous les onze jours. » Le gobe-mouche mâle, lui, ne met que trente-quatre minutes avant de s'accoupler avec une nouvelle femelle.

Consultons enfin l'index. Complet, il rend fidèlement compte du contenu du livre. Surprises : le mot plaisir, qui figure dans le titre, n'apparaît pas dans l'index ; des mots comme désir, érection, érotisme, excitation, jouissance, orgasme, volupté (pauvre Sainte-Beuve !) ne s'y trouvent pas non plus. Il y a tromperie sur la marchandise ! Cela dit, les philosophes aiment à rappeler que le mot chien ne mord pas : le signifiant n'est pas le signifié. De même, le sexe est troublant, mais la littérature érotique, en général, ne l'est pas. Alors, foin des regrets. Lisons *Pourquoi l'amour est un plaisir* dans la seule intention d'y apprendre des informations qui ne feront rougir personne.

Le pouvoir de l'image

Publier des photos prises dans la rue va être difficile, désormais. Les architectes, en effet, sont devenus très sourcilleux. Ils exigent des droits d'auteur quand on publie une photo où apparaît un monument construit par eux, fût-il public, et obtiennent gain de cause en justice (*Le Monde*, 27 mars 1999).

La veuve d'Otto von Spreckelsen, l'architecte de la grande arche de la Défense, est ainsi devenue la bête noire des producteurs d'images. Supposons, alors, que je déteste la grande arche de la Défense, et que je publie un ouvrage démontrant, photos à l'appui, combien elle défigure le quartier qu'elle domine de sa hauteur. Je devrai verser des droits à la veuve de l'architecte. Voilà une situation aussi cruelle que la double contrainte : on ne peut plus dire du mal d'une œuvre sans devoir lui apporter une contribution financière !

Triomphe suprême : vous contraignez vos ennemis à servir vos intérêts !

Les cadets de nos soucis

Avoir une idée intéressante, c'est facile (relativement). Résister au désir de lui assigner un rôle universel, c'est difficile. Ainsi, Frank Sulloway s'est demandé si le rang d'un individu dans sa fratrie influait sur son comportement. Ayant réuni une vaste documentation, il conclut que la plupart des innovations radicales ont été initiées et défendues par des cadets, alors que les aînés ont toujours eu tendance à rejeter les idées novatrices (Frank Sulloway, *Les enfants rebelles*, éditions Odile Jacob, 1999).

Soit. Last but not least, F. Sulloway donne à sa découverte un statut d'explication universelle. Cela le conduit à un réductionnisme qui fera sourire. Voici. « Leibniz et Newton étaient tous deux des aînés, ce qui permet de mieux comprendre la hargne dont ils firent preuve. Les premiers-nés n'aiment pas arriver en seconde position, et pour éviter une telle situation, ils sont prêts à sacrifier les règles du respect le plus élémentaire » (p. 100). « Nous avons tendance à considérer les monarques comme des individus conservateurs sur le plan social. La part de vérité contenue dans cette généralisation provient de ce que les rois et les reines sont souvent des aînés » (p. 129).

F. Sulloway explique même les luttes politiques par l'ordre de naissance. Ce dernier joue un rôle clé dans la Révolution française. « Au sein de la Convention nationale, les députés se groupèrent selon des tendances liées à des différences systématiques entre frères, les principales étant induites par l'influence de l'ordre de naissance » (p. 312).

L'auteur oublie qu'un individu peut être rebelle sur le plan social, mais conservateur sur le plan scientifique, ou l'inverse. Pour lui, les gens sont d'un bloc. Exemple. Tycho Brahe est mort pour n'avoir pas osé quitter la terre distinguée où il était reçu, alors qu'un besoin urgent le pressait. Cela prouve qu'il ne pouvait pas révolutionner les sciences : « Un homme incapable d'une entorse aux bonnes manières, fût-ce pour satisfaire un besoin naturel, n'était pas apte à défier les fondements de la cosmologie » (p. 27).

F. Sulloway omet de préciser son rang de naissance dans sa fratrie. Ce renseignement ne nous serait-il pas essentiel pour juger la pertinence de ses raisonnements ?

© POUR LA SCIENCE - N° 260 JUIN 1999

Fin de siècle

L'article de Peter de Jager *Les ordinateurs passeront l'an 2000* (voir *Pour la Science*, mars 1999) inventorie correctement la plupart des éléments du «bogue de l'an 2000», mais il en oublie un, qui a déjà eu des conséquences à la fin des années 1980 en Italie et que l'on retrouve aujourd'hui, à la fin des années 1990 : certains programmeurs ont utilisé une arithmétique des dates pour le moins approximative, qui fait que neuf plus un n'égale pas toujours dix. Il s'agirait peut-être là de la seule véritable erreur de programmation, alors que la terminologie «bogue de l'an 2000» suggère que tout y est erreur.

Notons au passage que, si les informations des temps révolus sont respectables en grande partie de la situation actuelle, il n'ont fait à l'époque que transposer une pratique bien antérieure à la naissance de l'ordinateur : le codage des années sur deux chiffres. J'ai ainsi récemment observé au Musée d'Orsay, dans une exposition consacrée à Stéphane Mallarmé, des enveloppes montrant des cachets postaux datant de la fin des années figurant sur deux chiffres uniquement.

Enfin, pourquoi ni les médias, en particulier la presse informatique, ni les grandes associations d'informatique n'ont-ils tiré le signal d'alarme en temps utile, c'est-à-dire il y a une dizaine d'années ? Est-ce parce qu'il ne s'agissait, en fait, ni d'urgence, que d'une «vulgaire» confusion de réintéressement, dans sans grand intérêt ?

Jean-François COLONNA, Palaiseau

Égarements et manipulation

Guillaume Lecoindre, dans sa mise en garde justifiée contre les activités de l'Université Interdisciplinaire de Paris (voir *Des scientifiques s'égarent...*, *Pour la Science*, mai 1999), fait part de sa «très grande surprise» devant la présence de mon nom parmi ceux des auteurs d'une série de conférences de l'UIP. Ma surprise a été plus grande encore : ayant accepté de participer à un débat organisé par le groupe protestant du temple de l'Étoile, c'est seulement lors de cette rencontre que j'ai constaté sa récupération par l'UIP. Les responsables du débat m'auraient-ils prévenus de leurs accointances que j'aurais refusé tout net cette invitation. Devant des stratégies aussi insidieuses, la méfiance ne s'impose que plus encore. Que G. Lecoindre n'assimile toutefois pas trop vite les positions antirationalistes et obscurantistes aux néces-

saires discussions critiques sur la nature et les limites de la rationalité scientifique.

Jean-Marc LÉVY-LEBLOND, Nice

Il y a quelques années, l'Institut Rockefeller a organisé un séminaire sur les OVNI et les extraterrestres en invitant différents scientifiques. Le séjour, entièrement pris en charge comme le voyage, était paradisiaque. Les chercheurs qui participèrent firent des interventions critiques, mais mesurées. Ils ne se rendirent compte qu'ils avaient été bernés qu'à la lecture du compte rendu.

La réunion qui exploitait savamment leur prudence : c'était un piège. Il faudrait que les organismes qui organisent de telles réunions soient réhabilités et que cette liste soit accessible aux chercheurs. Il ne s'agit évidemment pas d'interdire à un chercheur de collaborer, en connaissance de cause, avec ces organismes, mais seulement d'éviter les tromperies.

J. HARTONG, Strasbourg

Bernard d'Espagnat, Ilya Prigogine, Trinh Xuan Thuan et d'autres personnes citées par G. Lecoindre sont considérées par leurs pairs comme des scientifiques. Souhaiteraient-ils saper le fondement d'une science qu'ils ont servi toute leur vie et qui les a récompensés ? Ou sont-ils tous assez naïfs pour prêter la main à ce que je ne sais quel complot ? G. Lecoindre semble adopter la méthode philosophique. C'est une option intéressante. Il est trop facile d'insinuer que les prix Nobel sont jaloux du bon temps.

Enfin, plus généralement, l'association attaque dans un même élan «les églises et les sectes». Cette association n'est ni innocente ni fortuite. Elle est soutenue par deux dessins provocateurs, qui évoquent les caricatures anticléricales les plus accrues.

André THOMAS, Paris

La grande majorité de nos concitoyens pensent que la science peut et doit tout expliquer. Or la science ne donne pas le pourquoi des choses, mais seulement le comment. Ils constatent aussi que la science se trompe (pour le sang contaminé ou pour la vache folle) ou, du moins, qu'elle trébuche et met en péril sa crédibilité. En outre, les scientifiques manquent de modestie : rares sont ceux qui disent que la science ne décrit pas le réel mais seulement un modèle prédictif de certains aspects de la réalité. Si l'on ajoute que les disciplines pseudo-scientifiques donnent des explications absolues et définitives, sans hésitations, les personnes qui ont besoin d'être rassurées ne peuvent qu'être tentées par ces voies.

Jean-Louis BERNOU, Fresnes

La science est-elle matérialiste par nature ? La science est méthodologiquement matérialiste : elle n'a à enregistrer que les processus relevant de la matière et de l'énergie. Cela n'implique pas que la science explique tout aujourd'hui. Sur l'encore inexpliqué, soit on croit, comme Popper, aux prétentions du «matérialisme prometteur», et l'on reste matérialiste de bout en bout, soit on n'y croit pas et toutes les options restent ouvertes. Or, sans fixer à la science des limites *a priori*, il est très honnête de masquer les obstacles. Est-il raisonnable de croire qu'un jour tout aura été expliqué ?

Dominique LAPLANE, Paris

Réponse de Guillaume Lecoindre

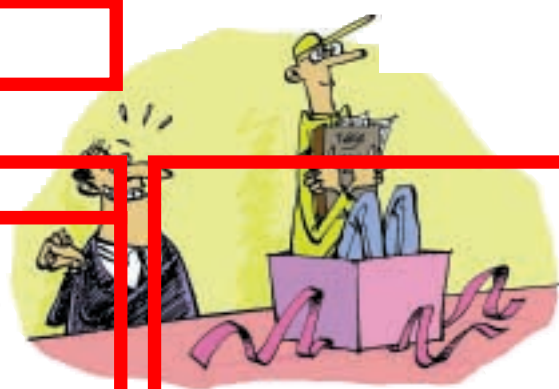
Des scientifiques reconnus de leurs pairs, qui ont basé leur brillante carrière à traiter du «complot», peuvent se faire manipuler : les lettres de J.-M. Lévy-Leblond et de J. Hartong le confirment. Antoine Danchin nous a aussi témoigné de sa grande surprise, dans les mêmes termes. Par ailleurs, des scientifiques reconnus peuvent déraiper, en utilisant leur science comme si elle confirmait les visions de leurs pulsions mystiques. Parfois même, ils utilisent le dictionnaire des sciences pour se faire passer pour des savants. Je suis un brillant mathématicien, académicien et membre de l'UIP qui parlait d'évolution dans certains journaux sans jamais rien y comprendre. Ce que je décris n'est pas un complot. Par ailleurs, je ne décale légèrement le thème, de manière à ce que son «paradigme» central soit déformé. Ce qui lui permet ensuite d'écrire que les scientifiques y souscrivent.

Que J.-L. Laplane et J.-L. Bernou veuillent bien remarquer que je n'ai jamais écrit que la science explique tout. Sur le front de la genèse des connaissances, le matérialisme reste sa seule condition méthodologique. Les autres options qui «restent ouvertes» consistent à sortir du champ de la science. Bien sûr, la science s'est toujours heurtée à des obstacles méthodologiques, il n'y a pas à le cacher. Ces obstacles stimulent l'invention de nouvelles méthodes scientifiques. Le fait que la science hésite ou se trompe fait partie du processus continu de la genèse des connaissances. Nous passons une bonne partie de notre temps à corriger des énoncés que nous découvrons être faux. Le sang contaminé et la vache folle n'ont que peu à voir avec la science en tant que démarche rationnelle de la découverte du monde. Ces deux catastrophes ne sont que des applications de la science, avec tout ce que cela comporte de facteurs économiques et politiques surajoutés, qui sont étrangers à la science dont je parle dans l'article.

La déformation par la recherche

BERNARD BEAUZAMY

Constant cruel : la thèse actuelle ne prépare guère ses détenteurs à travailler dans l'entreprise.



Les jeunes doctorants ont les plus grandes difficultés à trouver un emploi : les entreprises se méfient des thésards. Pour celui qui a fait une école d'ingénieurs au préalable, la thèse est un handicap (beaucoup s'efforcent de la dissimuler dans leur CV) ; pour celui qui a fait des études universitaires, elle ne laisse guère d'autre choix que l'enseignement et la recherche, toujours en milieu universitaire. Ces difficultés sont connues, et les candidats thésards sont rares : il y a peu de financements, encore moins de volontaires.

puis d'autres, formés ailleurs. Cela a toujours été la même catastrophe.

Les docteurs pensent retrouver, au sein de l'entreprise, une copie du laboratoire où ils ont préparé leur thèse : un sujet de recherche et quelqu'un pour les encadrer. En même temps, de manière paradoxale, ils voudraient «prendre des responsabilités», devenir chef de projet.

Comment le pourraient-ils ? Ils n'ont pas la moindre idée de ce que peut être une activité scientifique hors du monde académique. Pour nous, prestataires de services à l'industrie, un problème n'est jamais bien posé : nous passons des mois à discuter avec les responsables industriels pour comprendre ce qu'ils veulent.

Après quoi nous proposons une résolution partielle, la soumettons, recueillons les critiques et recommençons.

Les réunions, discussions, mises en question sont longues et difficiles. Et quand le congrès est terminé, il faut valoriser les résultats, les présenter, les rédiger sous forme exploitable, organiser des démonstrations, etc.

Que de difficultés pour le thésard, trop souvent incapable de présenter ses résultats hors des cercles académiques !

J'ai maintes fois fait l'expérience. J'ai interrogé des thésards sur leurs travaux. Je n'ai rien compris. Ils me disent qu'ils travaillent sur tel problème posé par Machin en 1992 (leur directeur de thèse), mais l'origine du problème, la pertinence de la question, la raison pour laquelle Machin l'a examinée en 1992, les thésards ne me l'ont pas expliquées.

Or un dirigeant d'entreprise souhaite que ses clients saisissent ce que font les ingénieurs, que le client comprenne à quoi sert la société qu'il dirige ; sinon, celle-ci ne vivra pas longtemps.

Comment confier des responsabilités à des gens dont le travail ne paie pas le salaire ? J'ai, comme nombre de chefs d'entreprise, bénéficié de subventions de l'ANVAR pour les recrutements ; ces

subventions prennent en charge la moitié de la masse salariale (masse salariale égale, dans mon cas à environ 220 000 francs par an) pendant la première année. Même avec ces subventions, les thésards couvraient à peine leur salaire. La raison : ils trouvaient un problème intéressant, se focalisaient dessus et y passaient tout leur temps. Qu'importe si le problème ne rapportait à l'entreprise que 50 000 francs !

L'État, qui a mis en place ces subventions, sait bien qu'un chercheur est peu rentable pour une entreprise, au moins les deux premières années. Sans doute finissent-ils par acquérir de bonnes habitudes et ne pas perdre les mauvaises... s'ils acceptent les contraintes de l'emploi.

PLUTÔT MOINE QU'UN PRÊTRE-OUVRIER...

Je m'interromps quelques instants dans la rédaction de cet article : l'une de mes thésards me demande de corriger le résumé anglais d'un article qu'elle veut soumettre à un congrès. Excellent. Il faut encourager la participation à des congrès. Toutefois, ne faudrait-il pas aussi présenter aux industriels les techniques que nous avons développées et qui sont susceptibles de les intéresser ?

Pourquoi un thésard est-il si désireux de participer à un congrès et souhaite-t-il si peu plancher devant le CEA ou l'ANVAR ? À participer à un congrès, on acquiert une notoriété, ce qui est flatteur pour l'égo. À plancher devant le CEA, on risque des rebuffades : les ingénieurs savent de quoi ils parlent et ne s'en laissent pas aisément conter. Les industriels ne feront appel à des méthodes nouvelles que si elles ont fait leurs preuves, si les algorithmes tournent en des temps raisonnables et donnent des résultats plausibles. Devant un congrès, on peut énoncer des hypothèses d'école, présenter des algorithmes qui mettent trois jours et donnent des résultats une fois sur deux.

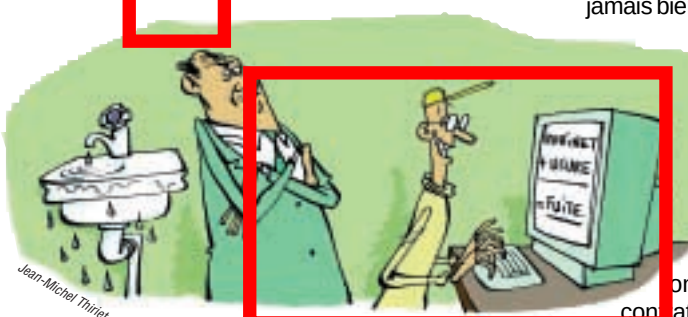
L'ingénieur est habitué à des solutions approximatives, voire fausses, mais il est

Pourtant, l'idée était séduisante : dans un monde scientifique en mutation, celui qui a été formé à la recherche, par la recherche, saurait mieux s'adapter que celui qui a appris des techniques toutes faites. Le chercheur serait plus souple, plus évolutif, plus curieux, plus disponible intellectuellement que l'ingénieur et, de ce fait, plus utile à l'entreprise.

Hélas, il n'en est rien. De trop nombreux chercheurs, tels qu'ils sont formés aujourd'hui, ne sont ni souples ni curieux, et sont trop souvent, à mon avis s'en rendant dépourvus des qualités dont une entreprise a besoin.

1 J'AI CRU

Professeur de l'Université, j'ai dirigé, en 20 ans, 22 thèses en mathématiques et disciplines connexes. En 1995, j'ai quitté l'Université pour monter mon entreprise. J'ai essayé d'employer des thésards, d'abord ceux que j'avais formés,



Jean-Michel Thiriet

familier des contraintes de temps, de rendement, de présentation, d'exploitation. Le thésard lui, désire des solutions parfaites : aussi sa solution est-elle presque toujours exploitable en l'état, et elle finit à la poubelle, alors même qu'il s'agissait parfois d'un début satisfaisant, qu'une ou plusieurs générations d'ingénieurs auraient pu ensuite transformer en un produit utilisable.

Les bourses CIFRE, qui requièrent la présence d'un industriel pour le financement et l'orientation de la thèse, sont mieux adaptées à la finalité de la recherche. Les employeurs ne s'y trompent pas et leur accordent la préférence : il y a peu de chômeurs parmi les anciens boursiers CIFRE.

Examinons brièvement – ce n'est pas l'essentiel de mon propos – le cas des mathématiques, singulières par deux aspects. D'une part, elles ont des débouchés constants liés à l'enseignement. D'autre part, les applications des mathématiques sont mal identifiées par les enseignants : ils s'imaginent que ces applications relèvent du calcul scientifique, de l'analyse numérique, alors que les débouchés de ces techniques sont insignifiants.

Pour résoudre un problème physique, par exemple prévoir les caractéristiques d'un écoulement, on a généralement recours à un procédé très ancien dénommé «discrétisation» : on écrit les équations qui régissent le problème et l'on se contente de calculer les valeurs des inconnues seulement en des points particuliers, par exemple tous les centimètres. De cette façon, on obtient un gros système linéaire facile à résoudre sur ordinateur. Cela fait 30 ans que la communauté académique considère que ce sont là les principales applications des mathématiques, et les trois quarts des jeunes formés en DEA, DESS ou thèse acceptent cette idée. Erreur funeste : il n'y a pratiquement pas de débouchés à cette formation. Le nombre de spécialistes nécessaires à l'utilisation de ces techniques est de plus en plus petit.

Imaginez-vous un étudiant en médecine qui, sitôt sa thèse terminée, va enseigner la médecine sans avoir jamais vu de

malade ? Imaginez-vous un jardinier qui va enseigner l'horticulture au lieu de ses étés des sans-jardin mais a toujours planté des fleurs ? Non ?

Eh bien, vous aurez quelque difficulté à imaginer qu'un mathématicien puisse enseigner les mathématiques sans les avoir jamais pratiquées. C'est pourtant ce qui se passe, c'est pourtant ce qui est la norme. Un jeune fait son DEA (Bac + 2) avec pour seul stage la lecture de quelques articles ; il passe sa thèse à l'Université, et ensuite il est recruté comme maître de conférences, puis devient professeur. Il va enseigner les mathématiques toute sa vie, sans jamais les avoir pratiquées. Inutile de dire que l'enseignement est bien coupé des réalités : aussi bien les réalités scientifiques et techniques que des besoins des entreprises ou de la société. On enseigne une version académique des mathématiques, une sorte de virtuosité virtuelle, où l'on «démontre» des résultats ; syllogismes dont les prémisses et le contexte ne sont pas toujours pertinents.

LA RECHERCHE : DU TEMPS PERDU ?

Le cas des thésards en mathématiques est donc particulier : ou bien ils se destinent à l'enseignement, ils y naissent, y vivent et y meurent (et je ne les vois pas), ou bien ils se destinent aux mathématiques appliquées et, outre les travers généraux de formation que j'ai décrits précédemment, ils ne savent pas travailler et ne savent pas où travailler, car ils ont une idée fautive des débouchés.

Les thésards des disciplines voisines (traitement du signal, télédétection, robotique, physique, mécanique, etc.) ont une meilleure idée du contenu de leur discipline, parce que celle-ci est en contact plus étroit avec les applications. Subsistent bien sûr, dans chacune de ces disciplines, des développements ineptes, des théories grotesques, des constructions absurdes, chacune avec sa cohorte de thésards qui soulignent l'importance du Maître.

Vieux débat sur l'inné et l'acquis : est-ce parce qu'ils sont réfractaires au monde réel que les jeunes deviennent thésards, ou bien sont-ils déformés par leurs années de thèse ?

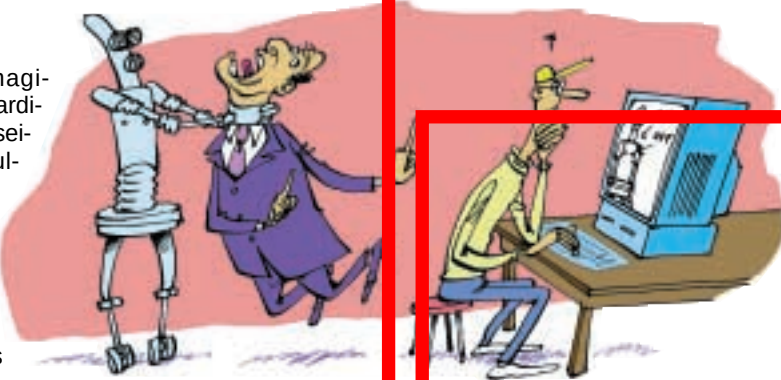
Je persiste à penser – vieux fonds d'optimisme ! – que la formation par la recherche est possible et qu'elle est

souhaitable dans le monde moderne. Ce qui est en cause, c'est le mode de jugement de la recherche, le «jugement par les pairs». Ce jugement privilégie la notoriété personnelle, au travers des publications, des congrès, au détriment des réalisations effectives. Le jugement par les pairs n'est pas inutile, et les publications sont utiles, mais l'objectif d'un programme de recherche, c'est avant tout le développement de nouvelles connaissances et leur mise à disposition auprès de ceux qui peuvent en avoir besoin. De ce point de vue, l'intérêt des publications, qui ne sont utiles que par un cercle restreint d'inités, est très faible.

Que le thésard se destine ensuite à l'enseignement ou à l'entreprise, peu importe, c'est son affaire, et les deux sont utiles. Ne serait-il pas souhaitable, cependant, qu'il pratique les mathématiques avant de les enseigner : les stages de DEA devraient être de vrais stages, hors du monde académique et, surtout, ils ne devraient pas être limités à la lecture d'articles. Ensuite, la thèse pourrait être faite en partenariat avec un organisme non académique qui a des programmes scientifiques de bonne qualité et doit obtenir des résultats.

Je voudrais terminer sur une note optimiste en sur un conseil personnel aux thésards. Les réticences que j'ai énoncées plus haut, beaucoup d'employeurs les ressentent et ils écartent la candidature des doctorants. Pourquoi ceux-ci, dans leur lettre de motivation, ne mentionneraient-ils pas qu'ils sont conscients de cette difficulté, par une phrase du type : «Je suis conscient que ma formation par la recherche ne m'a guère permis de connaître les réalités de l'entreprise, mais je suis tout prêt à les découvrir» ? Ils pourraient ajouter, et ceci à mon avis serait déterminant, qu'ils accepteraient une période de formation (mettons trois à six mois) à salaire réduit : une telle approche serait très séduisante pour l'employeur, qui verrait qu'il est en présence d'un candidat véritablement motivé.

Bernard BEAUZAMY est PDG de la Société de Calcul Mathématique, SA.





Les découvertes oubliées d'Alan Turing

JACK COPELAND • DIANE PROUDFOOT

Conçu pour la machine qui porte son nom, il fut aussi le père des réseaux de neurones.

Tous les ordinateurs actuels sont des descendants de la « machine de Turing » conçue en 1935 par Alan Mathison Turing. Ce mathématicien britannique fut également un pionnier de l'intelligence artificielle : il proposa un test — fameux, mais controversé — permettant de déterminer si un ordinateur « pense ». Au cours de la Seconde Guerre mondiale, il contribua à décrypter le code allemand *Enigma* dans le cadre d'une opération britannique secrète qui, d'après les historiens, abrégua de deux ans la guerre en Europe. Au moment de sa mort, à 41 ans, Turing travaillait sur ce que l'on nomme aujourd'hui la « vie artificielle » simulant la chimie de la croissance — de la morphogenèse.

Tout au long de sa carrière, Turing s'est peu préoccupé de faire connaître ses idées, de sorte que certains aspects de ses travaux sont passés inaperçus ou ont été oubliés. Rares sont ceux, même parmi les spécialistes de l'informatique, qui connaissent les travaux de Turing sur l'informatique « neuronale ». De surcroît, ses conceptions novatrices des « hyperordinateurs » n'ont pas été prises en compte : des spécialistes pensent que les hyperordinateurs de Turing pourront un jour résoudre des problèmes jugés insolubles aujourd'hui.

Les ordinateurs dévorent les nombres. En quelques secondes, ils calculent la trajectoire des fusées ou les résultats comptables des grandes sociétés. En revanche, la programmation des actions apparemment simples, que nous accomplissons sans même y penser, telles que reconnaître un visage ou lire un livre, est autrement difficile. Les réseaux de neurones du cerveau humain ont des capacités dont sont encore dépourvus les ordinateurs ; mais, les informaticiens tentent-ils de reproduire, par l'informatique, le fonctionnement du cerveau humain.

Le connexionnisme est cette nouvelle branche de l'informatique où les calculs sont effectués par des réseaux de neurones artificiels. Les informaticiens simulent les neurones et leurs

connexions sur des ordinateurs (tout comme les ingénieurs créent des modèles virtuels d'ailes d'avion ou de grattes-ciel). Un algorithme d'apprentissage ajuste les connexions entre neurones, pour que la machine, dédiée à une tâche précise, l'accomplisse de mieux en mieux.

Les connexionnistes modernes considèrent Frank Rosenblatt, qui publia le premier article sur le sujet en 1957, comme le fondateur de la discipline ; or, dès 1943, Turing avait étudié les réseaux de neurones dans un article intitulé *Intelligent Machinery*.

LA MACHINE DE TYPE B

Turing écrivit cet article alors qu'il travaillait au Laboratoire de physique de Londres. Considérant que l'article ne vaut guère mieux qu'une « dissertation d'écolier », son directeur, Charles Darwin — le petit-fils du naturaliste — le rejetta. En réalité, cet article visionnaire était le premier de tous ceux qui allaient être publiés sur l'intelligence artificielle. Dans ce manuscrit, qui ne fut publié qu'en 1968, 14 ans après sa mort, le mathématicien britannique formulait les principes du connexionnisme, et introduisait plusieurs concepts fondateurs de l'intelligence artificielle que d'autres redécouvrirent ultérieurement.

Dans cet article, Turing invente une sorte de réseau de neurones, qu'il dénomme « machine non organisée de type B » constituée de neurones artificiels et de dispositifs qui modifient leurs connexions. Les machines de type B incluent autant de neurones que l'on veut, connectés comme on veut, mais chaque connexion entre deux neurones passe par un dispositif modificateur.

Tous les modificateurs de connexions ont deux fibres d'apprentissage. Une impulsion sur l'une d'entre elles met le modificateur en « mode passage », dans lequel une entrée, soit 0 soit 1, traverse sans être modifiée et devient une sortie. Une impulsion sur l'autre fibre met

le modificateur en « mode interruption », où la sortie est toujours égale à 1, quelle que soit l'entrée. Dans cette configuration, le modificateur détruit toute information qui traverse la connexion à laquelle il est lié.

Une fois initialisé le modificateur conserve sa fonction (« passage » ou « interruption »), à moins qu'il ne reçoive une impulsion sur l'autre fibre d'apprentissage. Ces modificateurs de connexions, dont le principe est très astucieux, permettent à une machine non organisée de type B d'apprendre au moyen de ce que Turing appelait « des interférences appropriées », qui imitent les mécanismes éducatifs. Selon Turing, « le cortex d'un jeune enfant est une machine non organisée, qui se structure grâce à un entraînement approprié ».

Chaque neurone du modèle de Turing a deux fibres d'entrée, et la sortie est une fonction logique simple de ses deux entrées. Chaque neurone du réseau effectue la même opération logique suivante : si une des deux entrées est 0, la sortie est 1 ; si les deux entrées sont 1, la sortie est 0. Ces neurones sont de type NAND (le anglais *not and*).

Turing avait choisi ce type de porte parce que toutes les autres opérations logiques (ou booléennes) sont exécutables par des ensembles de neurones de ce type. De plus, il a montré que les modificateurs de connexions eux-mêmes peuvent être créés à partir de neurones NAND. Ainsi, Turing construisait un réseau constitué uniquement de neurones NAND et de leurs fibres de connexion, un modèle de connexion parmi les plus simples que l'on puisse imaginer.

En 1958, Rosenblatt définit le connexionnisme : « L'information est mémorisée sous la forme de nouvelles connexions, ou de canaux de transmission dans le système nerveux (ou par la création de conditions équivalentes à de nouvelles connexions) ». La destruction de connexions existantes peut être fonctionnellement équivalente à la création de nouvelles connexions ; aussi, pour

construire un réseau destiné à accomplir une tâche spécifique, les informaticiens peuvent partir d'un réseau qui aurait trop de connexions et en détruire certaines. Les machines de type B de Turing apprennent par création et destruction de connexions.

Initialement, les machines de type B contiennent des connexions inter-neuronales aléatoires dont les modificateurs ont été mis au hasard sur «passage» ou «interruption». Au cours de l'apprentissage, les connexions inutiles sont détruites par basculement sur le mode interruption des modificateurs qui neurs sont connectés. Inversement, en faisant

passer un modificateur du mode interruption au mode passage, on crée une nouvelle connexion. Ces inactivations et activations sélectives des connexions façonnent le réseau aléatoire initial en un réseau organisé pour une tâche donnée.

Turing étudia d'autres sortes de machines initialement non organisées : il rêvait de simuler un réseau neuronal et les mécanismes d'apprentissage à l'aide d'un ordinateur. Il voulait «laisser tourner le système pendant un bon moment et l'examiner ensuite, comme un inspecteur d'école, pour constater les progrès réalisés». Hélas, ses travaux venaient trop tôt : ce n'est qu'en 1954,

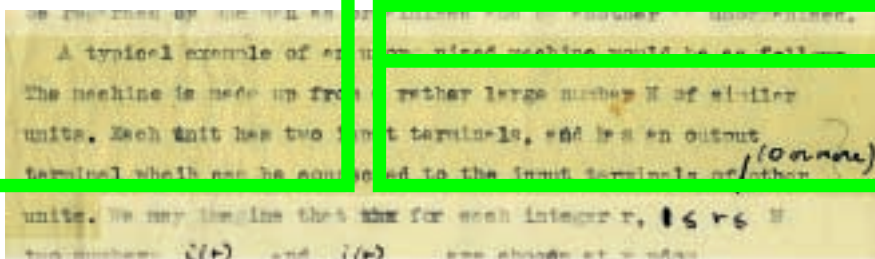
l'année de la mort de Turing, que Belmont Furlay et Wesley Clark réussirent la première simulation d'un petit réseau de neurones sur un ordinateur.

Un réseau spécialisé pouvait-il devenir universel ? Turing muni d'un crayon et de papier a montré qu'un réseau de neurones de type B suffisamment grand pouvait être configuré (grâce à des modificateurs de connexions) et devenir un ordinateur généraliste. Cette découverte éclairait l'un des principaux aspects de l'apprentissage humain.

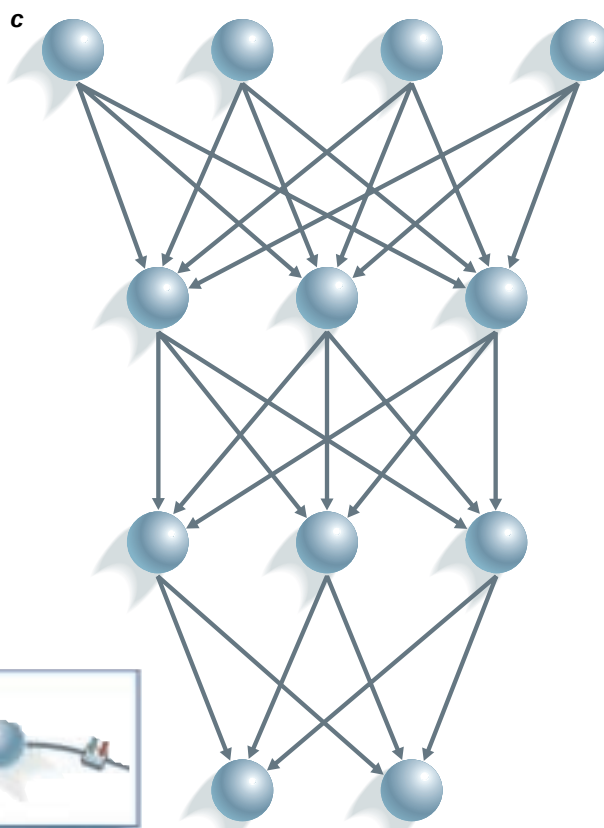
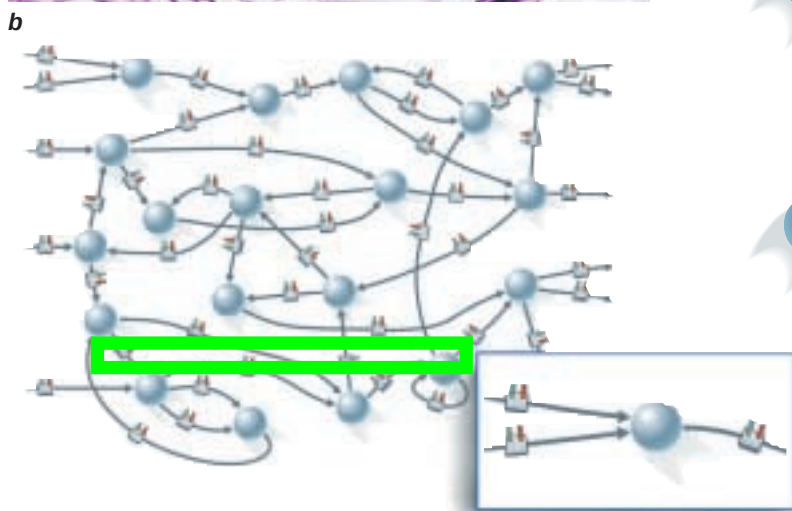
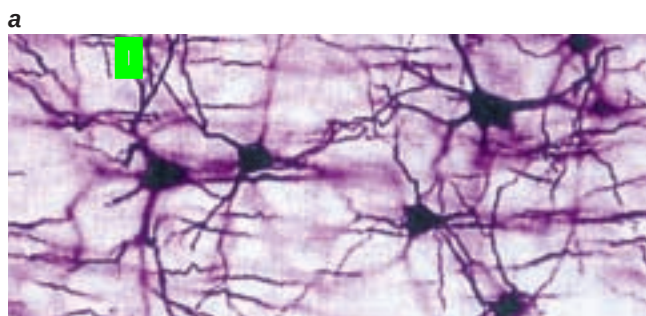
En effet, les mécanismes cognitifs sont séquentiels et complexes, faisant intervenir le langage ou d'autres formes

Turing et le connexionnisme

Dans un article qui ne fut publié que 14 ans après sa mort (ci-contre), Alan Turing décrivait un réseau de neurones artificiels connectés de façon aléatoire. Cherchant à reproduire les réseaux de neurones du cerveau (a), Turing a conçu une «machine inorganisée de type B» (b) : chaque connexion traverse un modificateur qui est réglé de façon à laisser passer la donnée inchangée (fiche verte), ou à détruire l'information transmise (fiche rouge). Le basculement des modificateurs d'un mode à un autre assure l'apprentissage du réseau. Chaque neurone a deux entrées (voir le cartouche) et exécute l'opération logique simple suivante : si les deux entrées sont 1, la sortie est 0 ; sinon la sortie est 1.



Dans le réseau de Turing les neurones s'interconnectent librement. En revanche, dans les réseaux modernes (c) le flux d'informations ne circule que d'une couche à l'autre.



L'oracle qui calcule l'incalculable

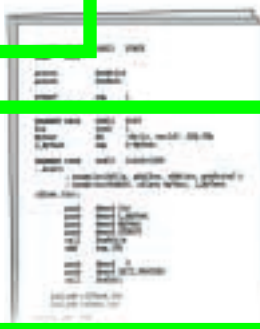
Alan Turing a démontré que sa machine universelle, et par conséquent, les ordinateurs les plus puissants, ne pourraient jamais résoudre certains problèmes. Par exemple, une machine de Turing ne peut pas toujours déterminer si un programme aboutira ou continuera à tourner indéfiniment. Dans certains cas, le mieux qu'une machine de Turing puisse faire est d'exécuter le programme et d'attendre, peut-être éternellement, qu'il se termine. Dans sa thèse de doctorat, Turing imaginait qu'une machine équipée d'un «oracle» pourrait remplir cette fonction et d'autres «calculs incalculables». L'exemple suivant illustre comment, en principe, pourrait fonctionner un oracle.

Considérons une machine hypothétique destinée à résoudre l'épineux problème de l'«arrêt des programmes». Un programme informatique peut être représenté comme une suite finie de 1 et de 0, suit qui peut s'interpréter comme la représentation binaire d'un nombre entier (par exemple 1011011 équivaut à 91). Le rôle de l'oracle serait défini ainsi : étant donné un entier qui représente un programme (pour tout ordinateur pouvant être simulé par une machine de Turing), le résultat sera 1 si le programme a une fin, sinon sera 0.

L'oracle serait un dispositif parfait de mesure et de stockage (une mémoire) contenant une valeur précise (appelons-la τ , comme Turing) d'une grandeur physique. La mémoire pourrait ressembler à un condensateur qui emmagasine

une quantité donnée d'électricité). En fait, τ serait une grandeur représentée par une suite infinie de chiffres binaires : 0,000000...1101... Le nombre τ aurait une propriété fondamentale : les chiffres qui le composeraient représenteraient précisément les programmes qui ont une fin et ceux qui n'en ont pas. Par exemple, si l'entier représentant un programme était 87 352, alors l'oracle pourrait calculer le 87 352^e chiffre de la suite binaire de τ (en comptant les chiffres décimaux de la gauche vers la droite après la

PROGRAMME INFORMATIQUE



100001.....001111

REPRÉSENTATION BINAIRE
DU PROGRAMME

de représentations symboliques, comme les formules dans les calculs mathématiques. Pourtant, les mécanismes cognitifs ne sont rien d'autres que des décharges de neurones. Les cogniciens sont confrontés à une question lancinante : comment faire converger ces deux approches ?

Turing avança une solution : le cortex est un réseau de neurones qui agit comme un ordinateur à usages multiples, capable d'accomplir les processus symboliques les plus abstraits. Cette affirmation, très en avance sur son temps en 1948, reste aujourd'hui encore parmi les meilleures réponses possibles à l'une des questions les plus ardues des sciences cognitives.

CALCULER L'INCALCULABLE...

En 1935, Turing invente le dispositif connu aujourd'hui sous le nom de «machine universelle de Turing». Elle est constituée d'une mémoire illimitée qui stocke à la fois le programme, les données et d'une tête de lecture-écriture qui parcourt la mémoire, symbole par symbole, lisant l'information et ajoutant de nouvelles données. Chaque instruction de base de la machine est très simple : par exemple «identifier le symbole sur lequel la tête de lecture est positionnée», «écrire le chiffre 1», «se décaler d'un cran vers la gauche». La complexité

naît de l'association d'un grand nombre de ces opérations de base. En dépit de sa simplicité, une machine de Turing peut exécuter les mêmes tâches que les plus puissants ordinateurs d'aujourd'hui. En fait, tous les ordinateurs modernes sont, par essence, des machines universelles de Turing.

En 1935, Turing voulait créer une machine, aussi simple que possible, et capable de faire les mêmes calculs qu'un mathématicien pourrait exécuter en utilisant une méthode algorithmique, sans limitation de temps, d'énergie, de papier ni de crayons et en étant parfaitement concentré. Cette capacité lui valut le qualificatif d'«universelle». Comme Turing l'écrivait lui-même, «Les ordinateurs sont conçus pour remplir n'importe quelle tâche d'un opérateur humain discipliné, mais dépourvu d'intelligence, pourrait accomplir».

Si puissants que soient ces ordinateurs, peut-on en concevoir de plus performants ? On peut effectivement décrire les «hyperordinateurs» sur le papier, mais personne ne sait si l'on pourra en construire un jour. Un nombre croissant d'informaticiens travaillent sur ces hyperordinateurs. Selon certains, le cerveau humain – le processeur le plus complexe que l'on connaisse – serait en fait un hyperordinateur naturel.

Avant que l'on s'intéresse aux hyperordinateurs, on pensait que tout problème de traitement d'informations

trop complexe pour une machine universelle de Turing était «incalculable». En ce sens, un hyperordinateur calcule l'incalculable.

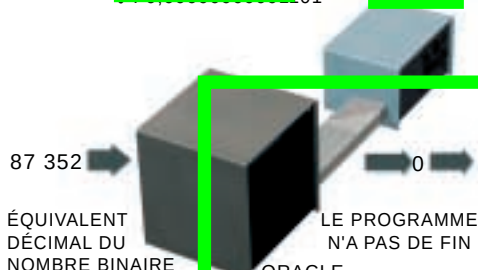
Certaines opérations paraissent défier les ordinateurs classiques même dans les domaines les plus élémentaires des mathématiques. Par exemple, quand on donne à une machine de Turing des propositions arithmétiques choisies au hasard, elle ne sait pas toujours distinguer ce qui est un théorème ($7+5=12$) de ce qui n'en est pas un (tout nombre est la somme de deux nombres pairs). Un autre problème incalculable est de nature géométrique. Avec un jeu de carrés de tailles différentes et dont des arêtes ont des couleurs différentes, on doit pavé le plan ; les carrés doivent se toucher (sans se superposer) et les arêtes adjacentes doivent être de même couleur. Les logiciens William Hanf et Dale Miller de l'Université de Hawaï ont découvert un jeu de carrés qui pave le plan, mais les motifs sont trop compliqués pour être calculés par une machine de Turing. Enfin, en informatique, une machine de Turing ne peut pas toujours prévoir si un programme aura

une fin ou s'il continuera à tourner sans fin. Aucun langage de programmation standard (Pascal, BASIC, Prolog, C,...) n'a d'outil qui détecterait tous les bogues risquant de faire échouer un programme, notamment les erreurs qui aboutissent à des boucles infinies.

virgule). Si c'était un 0, l'oracle conclurait que le programme tournera sans fin.

Évidemment, sans τ , l'oracle ne servirait à rien. On ne pourra peut-être jamais trouver un tel modèle mathématique. Pourtant, la quête de ce concept mathématique qui éclairerait la théorie de l'incalculabilité se poursuit.

MÉMOIRE D'ORACLE AVEC
PROCESSEUR 01



Turing a été le premier à rechercher des machines qui mèneraient à bien des tâches mathématiques trop compliquées pour la machine de Turing. En 1938, dans sa thèse de doctorat à l'Université de Princeton, il décrivait «un nouveau type de machine», la «machine O».

C'est une machine de Turing pourvue d'une boîte noire, ou «oracle», un dispositif qui exécuterait les tâches incalculables. Sinon, les machines O seraient identiques aux ordinateurs classiques. Un programme alimenterait la machine qui produirait une sortie numérique à partir de l'entrée, en utilisant un procédé itérant des opérations de base de la machine ; l'une d'entre elles consisterait à transmettre les données à l'oracle et à enregistrer sa réponse.

À LA RECHERCHE DE L'ORACLE

Turing ne donnait aucune indication sur le fonctionnement d'un oracle, pas plus qu'il n'avait expliqué, dans ses travaux antérieurs, comment une machine de Turing accomplissait ses fonctions de base, par exemple «identifier le symbole dans la tête de lecture». Toutefois, on peut en imaginer les principes fondateurs (voir l'encadré). En principe, même un réseau de type B adéquat pourrait calculer l'incalculable, à condition que l'activité des neurones soit désynchronisée : quand une horloge centrale

impose la même cadence à tous les neurones, le fonctionnement du réseau est parfaitement simulé par une machine universelle de Turing.

En théorie, les hyperordinateurs distingueront une proposition mathématique qui est un théorème d'une proposition qui n'en est pas un ; un correcteur de bogues pourrait même prévoir si un programme, quel que soit le langage dans lequel il est écrit, entrerait ou non dans une boucle infinie.

Si l'on parvenait un jour à construire des hyperordinateurs, on pourra résoudre d'innombrables problèmes de logique et de mathématique encore jugés insolubles. Le succès de l'entreprise tient essentiellement à une interrogation : réussira-t-on à concevoir un oracle ?

Des recherches sont menées tant en physique, qu'en chimie ou en biologie. Peut-être la solution viendra-t-elle de molécules complexes ou de structures qui s'arrangent selon des motifs compliqués. Ou bien, comme le pense Jon Doyle de l'Institut de technologie du Massachusetts, peut-être existe-t-il, dans la nature, des systèmes qui auraient un spectre discret, accompliraient des tâches incalculables, et produiraient des sorties appropriées (0 ou 1) après avoir été bombardées par le signal d'entrée.

Horrible, les logiciens, nul ne s'est intéressé aux machines O de Turing qui ont sombré dans l'oubli, et un mythe est apparu. D'après un récit apocryphe, Turing aurait démontré au milieu des années 1930 que les hyperordinateurs sont irréalisables. Avec le logicien Alonzo Church, son directeur de thèse à Princeton, il aurait énoncé un principe selon lequel une machine de Turing peut simuler le comportement de toute autre machine de traitement de l'information. Selon cette proposition, nommée à tort la «thèse de Church-Turing» (bien qu'ils n'en soient pas les auteurs), aucune machine ne peut traiter des informations que ne pourrait traiter une machine de Turing. En fait, Church et Turing affirmaient seulement qu'une machine de Turing pouvait remplacer n'importe quel mathématicien humain travaillant à une tâche précise, en utilisant et suivant une méthode algorithmique,

affirmation bien plus modérée et ne minimisant pas du tout les potentialités des hyperordinateurs.

Même ceux qui travaillent sur les hyperordinateurs n'accordent pas aux contributions théoriques innovantes de Turing la place qu'elles méritent. Les spécialistes parlent couramment de «dépasser la limite de Turing» pour le traitement des informations. On lit quelquefois que les nouvelles machines «vont bien au-delà des conceptions de Turing» et sont «des ordinateurs que jamais Turing n'avait imaginés», oubliant que le génie britannique avait élaboré le concept il y a plus de 50 ans. Il est dommage que les hyperordinateurs de Turing semblent devoir connaître le même sort que celui qu'ont connu ses idées sur le connexionisme d'oubli.

LES DERNIÈRES ANNÉES

À la fin de sa vie, au début des années 1950, Turing ouvrit un nouveau champ de recherches, celui de la vie artificielle. Il cherchait à simuler un mécanisme chimique où les gènes d'un œuf fécondé détermineraient la structure anatomique de l'animal ou de la plante à venir. Selon lui, ces recherches n'étaient pas sans rapport avec celles qu'il menait sur les réseaux de neurones, parce que «la structure du cerveau résulte nécessairement d'un mécanisme génétique d'embryogenèse et cette théorie, à laquelle je travaille actuellement, pourrait illustrer les contraintes que le mécanisme impose.» À cette époque, Turing fut le premier à explorer sur ordinateur les systèmes dynamiques non linéaires. Pour modéliser la chimie du développement, il utilisait des équations différentielles non linéaires.

Ainsi qu'il s'engageait dans tous ces domaines encore inexplorés, Turing souffrait d'un empoisonnement chronique ; il s'agissait probablement d'un suicide. Le 8 juin 1954, alors qu'il allait avoir 41 ans, on le retrouva mort dans sa chambre. Il laissait d'innombrables notes manuscrites et des programmes informatiques. Plusieurs dizaines d'années après, on ne les comprend pas encore tous.

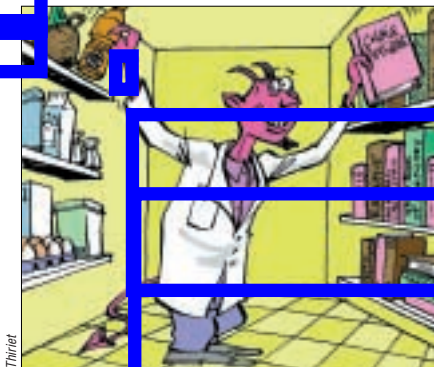
Jack COPELAND est professeur d'informatique à l'Université de Portsmouth. Diane PROUDFOOT est professeur de philosophie à l'Université de Canterbury, en Nouvelle-Zélande, où ils dirigent tous deux un Projet Turing qui développe les idées de Turing.

Hava SIEGELMANN, *Computation beyond the Turing Limit*, in *Science*, vol. 268, pp. 545-548, 28 avril 1995.

Alan TURING, Jean-Yves GIRARD, *La machine de Turing*, collection Points Sciences, Éditions du Seuil, 1995.

J. COPELAND, Diane PROUDFOOT, *On Alan Turing's Anticipation of Connectionism*, in *Synthese*, vol. 108, n° 3, pp. 361-377, mars 1996.

Jean LASSÈGUE, *Turing*, Collection Figures du savoir, Éditions Les Belles lettres, 1998.



Thiriet

Arômes ou réactions ?

HERVÉ THIS

Les chimistes identifient deux façons de donner du goût aux aliments.

Les choses doivent avoir le goût de ce qu'elles sont, disait le gastronomiste Curnonsky dans la première moitié du siècle. L'aphorisme a été adopté par de nombreux cuisiniers qui parlent aujourd'hui de «vérité» des goûts, mais est-il pertinent ? Le rôle du cuisinier n'est pas la transformation des produits alimentaires en vue de la confection des mets ?

Si l'objectif est l'obtention de goûts spécifiques comment communiquer ceux-ci aux plats ? Soit en ajoutant des arômes, soit en organisant des réactions chimiques, afin que les arômes soient formés *in situ*.

La technique la plus simple, mise en œuvre par l'industrie agro-alimentaire, est l'utilisation d'arômes, extraits naturels ou solutions de molécules de synthèse. Leur emploi en cuisine est simple (on verse quelques gouttes dans un plat), mais leur composition emploie des «nez», c'est-à-dire des artistes qui assemblent des solutions de diverses molécules aromatiques afin de reconstituer leur version de goûts connus : fraise, gingembre, romarin... Les cuisiniers hésitent à se laisser supplanter par ces «nez», d'autant que l'utilisation des produits naturels (du vrai thym et du vrai romarin dans une ratatouille, par exemple) donne souvent un résultat aromatiquement plus riche, et certainement plus varié, que l'utilisation d'un arôme industriel de thym ou de romarin (les «nez» n'assemblent généralement pas autant de molécules aromatiques qu'il en existe dans les produits naturels).

Doit-on pour autant écarter les arômes ? Ce serait perdre une occasion d'élargir la palette des goûts. Pourquoi ne renforcerait-on pas la note «verte» d'une huile d'olive avec de l'hexanal ? Pourquoi n'ajouterait-on pas du 1-octène-3-ol à un plat de viande afin de lui donner un arôme de champignons ou de sous-bois (attention au dosage : en concentration excessive, la même molécule sent un peu le mois) ? Pourquoi n'emploierait-on pas de la bêta ionone afin de donner aux desserts cet étonnant

arôme de violette que les fleurs ont bien du mal à libérer ?

D'autre part, pour donner de la saveur, et non de l'arôme, le cuisinier pourra employer le monod glutamate de sodium ou des molécules analogues, qui donnent la saveur nommée «umami», également apportée par les oignons ou par les tomates. Il pourra utiliser la réglisse ou l'acide glycyrrhizique, qui communiquent une saveur spécifique, qui n'est ni salée, ni sucrée, ni acide, ni amère.

Les progrès culinaires seraient-ils limités à cet avenir de l'aromatisation, qui s'apparente à l'ajout de fines herbes ou d'épices ? Certainement pas : le cuisinier sait bien que la cuisson transforme le goût de ses produits. Le feu est son allié inséparable, et la chimie peut l'aider à l'utiliser.

Par exemple, nous avons proposé dans cette rubrique, il y a quelques mois, la confection de caramels de glucose, de fructose ou, plus généralement, d'autres sucres que le saccharose (le sucre de table). Une expérience que chacun peut réaliser montre que ces caramels sont peut-être déjà présents en cuisine.

L'expérience se fonde sur une remarque apparemment paradoxale de cuisiniers : pour préparer des sauces, mettre dans une casserole des échalotes hachées et du vin blanc, qu'ils font réduire «à sec». Or certains vins blancs ne laissent aucun résidu dans les casseroles. Pourquoi ? Parce qu'il leur manque du glucose, du glycérol et bien d'autres constituants. Conclusion pratique : si le vin blanc risque de s'évaporer excessivement, ajoutons-lui du glucose avant de réduire... et nous obtiendrons ce caramel de glucose qui contribue au goût des vins réduits à sec.

Cette réduction, même ainsi épaulée, reste étonnante : pourquoi évaporer l'essentiel des molécules aromatiques qui sont présentes dans les vins ? La question se pose également dans le cas des fonds, que les cuisiniers obtiennent en

concentrant des bouillons de viande par chauffage. Si la concentration élimine les molécules aromatiques, pourquoi les fonds sont-ils néanmoins savoureux et parfumés ?

Anthony Blake et François Benzi, de la Société Firmenich, ont comparé par chromatographie un bouillon réduit des trois quarts, puis ramené à son volume initial par ajout d'eau au même bouillon non modifié. La concentration en certains composés aromatiques était effectivement réduite, mais d'autres composés étaient nés des réactions, favorisées par l'échauffement, entre les divers constituants du bouillon. Reste à identifier ces réactions afin de perfectionner – qui sait ? – la confection des fonds.

Les possibilités de la chimie sont innombrables : nous avons sur nos étagères de cuisine une foule de produits quasi purs : chlorure de sodium, saccharose, triglycérides (dans l'huile), éthanol, acide acétique, etc. ; et, dans nos bibliothèques, des traités de chimie décrivent parfaitement les réactions de ces molécules. Ne pourrions-nous faire aujourd'hui la synthèse ?

Ainsi les réactions dites de Maillard, entre les acides aminés et les sucres, engendrent les composés goûteux et bruns de la croûte du rôti, du pain, les arômes du café ou du chocolat... Or les chimistes savent que ces réactions diffèrent selon l'acidité du milieu réactionnel. Trempons-nous un jour les suprêmes de volaille dans du vinaigre ou dans du bicarbonate de soude avant de les passer sous le grill, créant ainsi des goûts nouveaux ? Pour retrouver une acidité de dégustation appropriée, une fois la réaction effectuée, on neutraliserait le vinaigre au bicarbonate ou inversement...

Prochain rendez-vous France Info et Pour la Science le 30 juin 1999, avec la chronique Info Sciences de Marie-Odile Monchicourt.

PERSPECTIVES SCIENTIFIQUES

L'astronome astrologue

Un thème astral rédigé par Johannes Kepler a été retrouvé en Californie.

L'astronomie au XVI^e et au XVII^e siècle ne nourrissait pas son savant. L'astronome allemand Johannes Kepler (1571-1630) est connu pour ses trois lois sur le mouvement des planètes. Un manuscrit découvert récemment dans les archives de l'Université de Californie par Anthony Misch, astronome à l'Observatoire Lick, montre que Kepler s'adonnait également à l'astrologie afin d'arrondir ses fins de mois.

Grâce aux mesures précises effectuées par son maître l'astronome danois Tycho Brahe (1546-1601), Kepler a

découvert que les planètes décrivent des orbites elliptiques dont un des foyers est le Soleil ; que le rayon joignant le Soleil à une planète balaye une aire proportionnelle au temps ; et que le carré du temps de révolution d'une planète est proportionnel au cube du grand axe de l'ellipse parcourue. Ces lois qui l'ont fait passer à la postérité n'ont pas apporté la richesse à leur auteur.

La vie quotidienne de l'astronome royal à la cour du roi Rodolphe II de Habsbourg n'était pas facile ; elle était pire quand régna son fils Mathias II qui appréciait moins les sciences. Pour percevoir son traitement, Kepler, devait obtenir un document officiel, puis parcourir des dizaines de kilomètres jusqu'à une administration de province où il recevait enfin son argent. Les retards s'accumulaient. C'est en allant chercher une grosse somme d'argent que le roi lui devait, que Kepler contracta, à Ratisbonne, une maladie qui lui fut fatale.

L'astronome composait occasionnellement des horoscopes pour bénéficier de revenus supplémentaires. C'est ainsi qu'il dressa la carte du ciel astral de la naissance d'un noble autrichien. Sur le recto du manuscrit (voir les figures), de 20 centimètres de longueur et 15 centimètres de largeur, est écrit d'une main encore inconnue : «*En l'an de grâce 1586, le 10 septembre, à 17 heures, Hans Hannibal Hütter von Hütterhofen vint au*

monde... Suit alors un graphe rectangulaire dessiné par Kepler, qui représente la position des planètes dans les 12 divisions du ciel nommées maisons, au moment de la naissance. Cette représentation rectangulaire reste fréquente en Inde du Nord ; les astrologues occidentaux ont préféré une carte du ciel circulaire. La traduction est aisée, car les signes et les symboles utilisés sont restés inchangés pour représenter les constellations du zodiaque.

L'ascendant de Hans Hannibal Hütter von Hütterhofen, c'est-à-dire la constellation qui se levait au moment de sa naissance, était le Verseau.

En bas à droite, on lit : «*L'en-tête est d'une main étrangère, ce qui suit est écrit par Kepler. De la collection de manuscrits de Kepler à Pulkovo. Signé W. Struve, Pulkovo, 23 mai 1864*». Pulkovo est le nom d'un observatoire situé près de Saint Pétersbourg et fondé au début du XIX^e siècle par l'astronome russe Wilhelm von Struve (1793-1864). La date du commentaire coïncide avec la mort de Struve.

Le fils de Struve, dont les initiales sont les mêmes que celles de son père, et auquel il succéda à l'Observatoire de Pulkovo, est peut-être l'auteur de cette annotation. Les manuscrits de Kepler que mentionne Struve, rassemblés par ordre de Catherine II de Russie en 1773, sont aujourd'hui conservés à l'Académie de Saint-Petersbourg.

Comment ce manuscrit, conservé en Russie, est-il arrivé en Californie ? Dans un article publié en 1896, le premier directeur de l'Observatoire Lick évoque la mise en vente du manuscrit en Allemagne. L'Observatoire Lick s'en est porté acquéreur.

À l'époque de Kepler, l'astrologie, bien que bannie par l'Église, qui y voyait une limitation de l'autorité divine, était très répandue dans les cours d'Europe, non pas à des fins prédictives et superstitieuses, mais à des fins politiques. Plutôt que de laisser les prédictions, bonnes ou mauvaises — se répandre anarchiquement parmi la population, les monarques préféraient contrôler ce moyen d'influencer l'opinion publique. Kepler ne croyait pas à l'astrologie, mais il était persuadé que l'ordonnement de l'univers avait un effet sur la vie quotidienne.

Les temps ont bien changé : la communauté des astrologues est aujourd'hui bien distincte de celle des astronomes. Est-ce parce que ces derniers sont payés plus régulièrement ?

Sur le recto du manuscrit de Kepler (en bas) figurent un en-tête d'une main inconnue, une carte du ciel dessinée par Kepler et un commentaire de l'astronome Wilhelm von Struve (en bas à droite). Le verso du manuscrit (en haut) porte les positions des planètes.

L'amour est aveugle

Même aveugles, les serpents tiges parviennent à se nourrir et à trouver leurs partenaires.

L'intégrité des organes sensoriels est-elle indispensable à la survie des animaux ? Les chamois ou les koalas meurent rapidement lorsqu'ils sont aveuglés au cours d'épizooties de kératite conjonctivite, et l'on imagine mal que des prédateurs aveugles, lions ou rapaces, puissent survivre. La perte de la vision (ou d'autres sens) peut être graduelle et être le cas pour les espèces qui ont progressivement évolué vers des habitats troglodytes (certains insectes ou poissons cavernicoles, par exemple), mais il est difficile de concevoir qu'une perte soudaine de la vision n'ait qu'un faible impact sur les organismes. Pourtant nous avons observé que des serpents aveugles peuvent survivre.

L'erpétologue américain Carl Gans a proposé, il y a 20 ans, une théorie qui complète la pensée classique et gradualiste des processus évolutifs : il existerait des situations écologiques dans lesquelles les organismes sont « sur-équipés ». Des individus plongés dans un environnement modifié auraient des capacités sensorielles superflues, lesquelles pourraient disparaître sans dommages pour l'individu.

Cette théorie est très difficile à vérifier dans les conditions naturelles : les animaux gravement mutilés (accidentellement aveuglés, sourds...) sont condamnés à court terme. Toutefois, les résultats que nous avons récemment obtenus sur les serpents apportent des éléments à la thèse du sur-

équipement. En 1997, en collaboration avec des collègues australiens, nous avons mis en place une étude de terrain sur les serpents tiges (*Notechis scutatus*) de l'île de Carnac, au large de Perth, en Australie occidentale. L'histoire de cette population, estimée à plus de 350 adultes, est assez particulière. Les serpents tiges de Carnac sont les descendants de 50 individus capturés dans la région de Perth, donc issus du continent, mais relâchés sur l'île, il y a 70 ans, par les autorités qui avaient confisqué les animaux d'un forain nommé Rocky Wale. Ce dernier organisait des spectacles avec les serpents, mais ceux-ci tuèrent la femme (et l'un de ses collaborateurs quelques années avant), d'où la confiscation.

Dès les premières captures, nous avons été surpris d'observer la fréquence élevée des individus qui présentaient des cicatrices sur le dos et sur la tête sur un total de 212 serpents tiges individuellement marqués, seuls 46 étaient intacts. Ce caractère inhabituel a été confirmé par l'observation de serpents tiges capturés à proximité de Perth et dans d'autres régions de l'Australie : tous étaient intacts. Parmi les serpents insulaires, 14 étaient borgnes et 16 autres totalement aveugles. Les cicatrices et les blessures, parfois encore sanguinolentes, attestent le caractère accidentel des lésions.

Nous avons identifié les causes des blessures en observant les comportements alimentaires. Les serpents tiges se nourrissent des poussins des mouettes argentées (*Larus novaehollandiae*) qui nichent en colonies sur Carnac. Les oiseaux défendent vigou-

reusement leur progéniture en infligeant des coups de bec aux serpents. Bien que les mouettes aient extrêmement peur des serpents (à raison), leurs comportements parentaux dominent et les incitent à prendre des risques élevés. Apparemment, les serpents tiges aveugles ne semblaient pas affectés par leur mutilation. Au contraire, ils sont en moyenne plus grands que les autres.

Une seconde mission, en 2000, nous a permis de recapter la plupart d'entre eux, montrant qu'ils avaient parfaitement survécu. Leur croissance en longueur, ainsi que leur prise de masse annuelles (des indicateurs directs de leur succès alimentaire) sont tout à fait normales. Ces résultats démontrent que les serpents tiges aveugles

BRÈVES

Le recul de la forêt

Proconsul, l'un des derniers ancêtres communs des grands singes supérieurs et de l'homme, vivait dans un milieu relativement sec. Erik Bestland, de l'Université de l'Idaho, et Evelyn Krull, de l'Université de l'Oregon, ont analysé les sols de 18 millions d'années de l'île de Lusinga, sur le lac Victoria, au Kenya contenant de nombreux fossiles de *Proconsul*. La zone, fréquemment dévastée par les éruptions du volcan Kisingiri tout proche, était couverte d'une forêt très ouverte. Contrairement à ce que laissent supposer les analyses antérieures de pollens, la forêt dense et humide n'occupait que des espaces restreints.



Alan Walker

Trous noirs créant une galaxie

En observant des radiosources puissantes, une équipe d'astronomes hollandais et américains a découvert la plus lointaine, donc la plus ancienne, galaxie connue ayant en son centre un trou noir : elle existait quand l'Univers n'avait guère plus d'un milliard d'années. On pensait qu'un trou noir massif se construisait à partir d'une grande quantité de matière galactique. Mais, en fait, bref, un trou noir ne peut se former. Cette observation favoriserait un autre scénario de formation des galaxies : de petits trous noirs primordiaux coalesceraient en un noyau proto-galactique qui attirerait le gaz et la poussière environnante pour donner une galaxie analogue à celle qui a été découverte.

Les OGM et les papillons

La transformation génétique des organismes végétaux évite l'emploi de pesticides, mais elle affecte les papillons : John Losey et ses collègues de l'Université Cornell ont étudié le développement de la chenille du papillon (*Pieris plexippus*) sur des feuilles de maïs où ils avaient dispersé le pollen de maïs transgénique. Ce maïs contient un gène du bacille *Bacillus thuringiensis* qui fait produire à la plante une toxine repoussant les ravageurs. Sur les feuilles pollinisées, les larves du papillon se développent très lentement, et leur mortalité est supérieure à la normale.



Xavier Bonnet

Un nouvel anticoagulant

L'héparine est le plus utilisé des anticoagulants. Après chaque opération chirurgicale, elle est injectée au patient pour diminuer le risque de thrombose. Cette molécule, composée d'une trentaine de sucres, a toutefois des effets secondaires : elle provoque des hémorragies. Des chercheurs de l'université de Paris-Saclay et de l'Institut Pasteur ont mis au point une molécule analogue à l'héparine, mais composée de seulement 17 molécules de sucres. Apparemment dénuée d'effets secondaires, son activité antithrombotique est dix fois supérieure. Les premiers essais cliniques sont prévus en 2020.

Extinction des feux!

Les enfants de moins de deux ans dont la chambre est éclairée pendant la nuit risqueraient plus que les autres de devenir myopes. C'est ce qu'établit une enquête menée auprès des parents de 479 enfants par des ophtalmologues de Philadelphie. Les enfants dont la chambre est la plus grande et la plus lumineuse ont subi une baisse de vision plus importante. Parmi les enfants étudiés, 48 pour cent de ceux qui avaient dormi avec une lumière artificielle étaient devenus myopes, contre seulement 31 pour cent de ceux qui n'avaient subi que la lumière d'une veilleuse, et 9 pour cent de ceux qui avaient dormi dans l'obscurité complète.

Faire la grosse voix

Pourquoi de nombreux oiseaux ont-ils une gorge si grande ? Une étude menée par des chercheurs de l'université de Californie a permis de répondre à cette question. Les chercheurs ont découvert que la gorge joue le rôle de caisse de résonance et que plus elle est longue, plus le son est grave. Un son caverneux est associé à un individu de grande taille : il effraie les prédateurs et aguche les futurs conjoints.

Libertins

Les archéologues, qui restaurent actuellement le palais impérial de Néron, ont découvert un caractère libertin : les signatures de Sade et de Casanova. Sade, qui séjourna à Rome en 1772 se serait arrêté au même endroit que Casanova, qui y était, lui, en 1770. Attirés ou inspirés?



sont « aussi bons chasseurs que leur congénères «intacts». Nous avons équipé de émetteurs deux mâles aveugles et tous les deux ont réussi à trouver une femelle et à s'accoupler. La perte de la vue n'a pas eu de conséquence détectable sur ces prédateurs.

Dans le lac Milieu d'origine (le lac de la Vierge), les serpents tiges chassent à vue des amphibiens qui constituent l'essentiel de leur régime alimentaire. Sur Carnac, tout est différent : il n'y a pas de lac, ni de point d'eau, et les amphibiens y sont totalement absents. Les serpents tiges ont su s'adapter à leur nouvel environnement et y survivent malgré la perte soudaine de vision.

Cette performance est liée à la combinaison d'un ensemble de facteurs. Les serpents tiges sont des animaux très pratiques : ils sont capables de tolérer des perturbations physiologiques importantes (par exemple, des jeûnes très longs plus d'un an parfois) et d'adopter des tailles ou des vitesses de croissance très variables, ce qui leur permet de s'adapter à leur environnement (par exemple, pour s'«ajuster» aux proies disponibles).

Sur Carnac, les proies – des milliers de vers de terre nichant au sol – sont faciles à capturer. De plus, la densité de serpents facilite les rencontres entre les sexes. Enfin, il n'y a pas de prédateurs, au moins pour les adultes. Dans ces conditions écologiques exceptionnelles, la vue est superflue : les serpents sont de fins limiers, qui utilisent à la fois leur odorant (narines, épithélium olfactif, bulbe olfactif), ainsi que leur système voméronasal (langue, organe de Jacobson situé dans le palais, bulbe olfactif accessoire).

Le second système sensoriel (absent chez les oiseaux et chez les mammifères) est extrêmement performant : le serpent compare simultanément les informations chimiques collectées par chaque brin de sa langue bifide et s'oriente ainsi avec précision. Les serpents tiges aveugles trouvent facilement leurs proies et leurs partenaires sexuels en suivant des pistes olfactives. Ils étaient bien équipés pour les nouvelles conditions de vie.

Curieusement, le nom du serpent tige, *Coluber constrictor*, fait référence à une écaille en forme d'écusson qui est située sur le crâne. C'est la cible principale des becs des mouettes, et l'évolution produira peut-être des serpents munis d'un bouclier faisant office de casque.

Xavier BONNET, Conseil général des Deux-Sèvres, Don BRADSHAW, Université d'Australie occidentale, Richard SHINE, Université de Sydney.

Un très vieux atelier

Il y a 2,34 millions d'années, la taille de la pierre était déjà perfectionnée.

Contrairement au vieil adage selon lequel «l'outil fait l'homme», ce dernier n'en a peut-être pas été le premier fabricant. Les archéologues ont mis au jour, depuis une vingtaine d'années, des outils taillés il y a 2,6 millions d'années, avant l'apparition probable de la première espèce du genre *Homo*. La découverte récente d'un «atelier de taille» de 2,34 millions d'années a permis notre perception de ces premiers tailleurs de pierre, qui ont fait preuve d'un étendu savoir-faire.

La taille des roches par des groupes d'hominiés, dès la fin de l'ère tertiaire, semble cantonnée à la moitié Nord du Rift Est africain. Une douzaine de sites y ont été découverts et fouillés. La formation de Hadar, dans le Nord de l'Éthiopie, a livré les plus anciens, datés de 2,6 à 2,5 millions d'années. Dans le bassin du Turkana, les sites de l'Ouest, au Sud de l'Éthiopie, et ceux de la formation de Nachukui, au Kenya, sont un peu plus récents : 2,4 à 2,3 millions d'années.

C'est dans la formation de Nachukui que nous avons fouillé, avec nos collègues du Projet archéologique de l'Ouest Turkana, le site de Lokalele 2C, un «atelier de taille» d'environ 20 mètres carrés. L'échelle chronologique régionale, établie à partir de l'empilement des couches de sédiments lacustres et fluviaux et de cendres volcaniques, a permis de dater ce site de 2,34 millions d'années. À cette époque, le bassin du Turkana était traversé par un fleuve où se jetaient des rivières temporaires, issues d'un massif montagneux bordant le bassin, à l'Ouest. C'est dans une ancienne plaine d'inondation à la confluence d'une de ces rivières et du fleuve, qu'un groupe d'hominiés s'est installé et a taillé la pierre pour en tirer des éclats coupants.

Tous les vestiges de cette activité ont été abandonnés sur place : des nucléus (blocs de matière première dont on tire des éclats), des éclats des galets et de petits blocs bruts en attente d'être taillés, ainsi que des perçuteurs. Environ 60 blocs de roches volcaniques diverses, probablement charriés par les cours d'eau voisins, ont été débités. Les blocs provenant de roches au grain le plus fin ont fourni de longues séries d'éclats (plus d'une trentaine dans certains cas), tandis que les blocs de moins bonne

qualité n'ont servi qu'à la production de quelques éclats. Les tailleurs de pierre ont donc exploité de préférence les roches les plus « taillables » et fournissant les éclats aux tranchants les plus acérés.

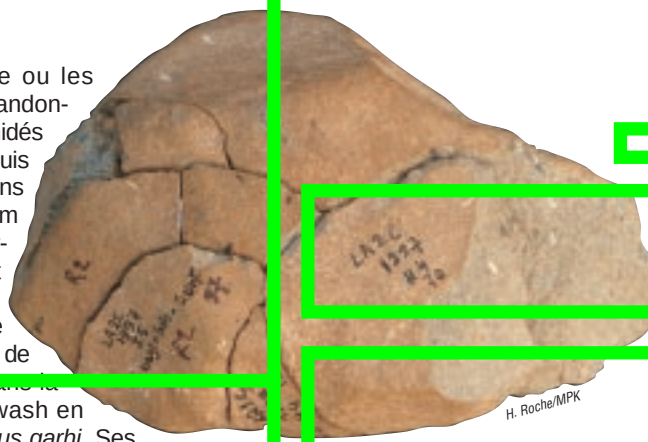
Grâce à l'exceptionnelle conservation de cet ensemble, nous avons reconstitué la plupart des blocs taillés, dont certains totalement en recollant les éléments qui en avaient été détachés. Ces remontages offrent la possibilité, unique pour un site aussi ancien, de retracer tout le processus qui va du bloc brut au nucléus abandonné. Le débitage a presque toujours été réalisé selon le même schéma opératoire : tous les éclats sont enlevés de la même face du nucléus, par percussion sur un replat naturel ou préparé. Cette technique exploite judicieusement la forme naturelle des blocs. Tout au long du débitage, des angles de frappe adéquats pour détacher des éclats sont conservés. Ce type de débitage, qui requiert une bonne précision motrice, indique une élaboration technique supérieure à celle que l'on connaissait dans les sites du même âge.

Qui a taillé si astucieusement ces outils ? Plusieurs espèces d'hominidés sont

candidates. Lorsque le ou les tailleurs de Lokalalei abandonnent leurs outils, des hominidés taillent déjà la pierre depuis au moins 200 000 ans dans la savane Est-africaine. Tim White, de l'Université Harvard, et ses collègues ont récemment annoncé la découverte d'une nouvelle espèce d'australopithèque de 2,5 millions d'années dans la moyenne vallée de l'Awash en Éthiopie : *Australopithecus garhi*. Ses restes étaient accompagnés d'os de mammifères portant des traces de découpe, et d'autres os longs écrasés par percussion, peut-être pour en extraire la moelle.

Bien qu'on n'ait pas retrouvé d'outils associés à cette espèce, *Australopithecus garhi* en a peut-être utilisés, voire fabriqués.

Par ailleurs, le plus ancien fossile connu d'un ancêtre direct de l'homme, *Homo habilis*, découvert aussi dans la vallée de l'Awash, date de 2,3 millions d'années. *Homo habilis* semble toutefois arriver plus tard dans le bassin de Turkana, tandis qu'une forme robuste d'australopithèque



Plusieurs éclats ont été détachés, il y a 2,3 millions d'années, de ce bloc de roche volcanique d'une dizaine de centimètres de long. La méthode de taille est étonnamment parfaite pour cette époque ancienne.

est présente dès 2,3 millions d'années. Pendant la longue période qui précède l'apparition du *Homo habilis*, il y a 1,6 millions d'années, on observe une diversité des compétences techniques. Plusieurs espèces ont-elles taillé la pierre ?

H. ROCHE et A. DELAGNES, CNRS, Préhistoire et technologie, Nanterre

Turbulence et transition de phase

La transition vers la turbulence ressemble parfois à la transition de phase du type liquide-gaz.

Les mouvements de fluide, que ce soit les écoulements de l'air dans l'atmosphère, autour du fuselage d'un avion, ou les écoulements des liquides dans les circuits de refroidissement, sont tantôt laminaires (calmes et réguliers), tantôt turbulents (désordonnés et aléatoires). Comment s'effectue le passage d'un régime à l'autre ? Dans un écoulement de cisaillement, nous avons mis en évidence la coexistence et l'intermittence entre un régime laminaire et un régime turbulent.

Les écoulements de fluide sont caractérisés par un nombre sans dimension, le nombre de Reynolds. Ce nombre est égal à la vitesse du fluide multipliée par la taille caractéristique de l'écoulement et divisée par la viscosité du fluide en mouvement. Dans un petit tube, où la vitesse d'un fluide très visqueux est faible, le nombre de Reynolds est petit, et l'écoulement est laminaire. Les deux autres paramètres étant constants, l'écoulement devient turbulent quand on augmente

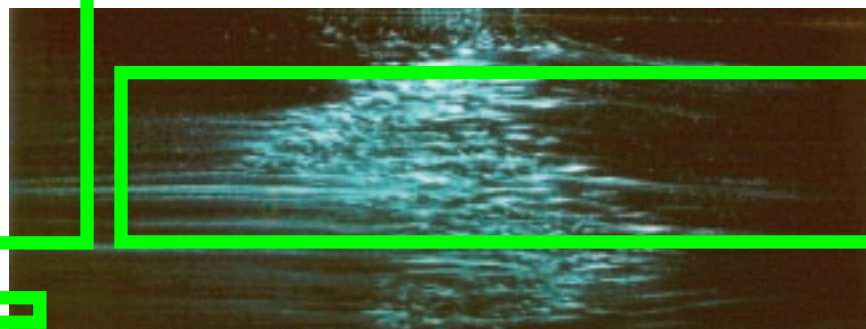
la vitesse du fluide. C'est la transition vers la turbulence.

Les transitions vers la turbulence sont de deux types : progressives ou brusques. Dans les transitions progressives, telles celles des jets ou des sillages, la turbulence apparaît dans tout l'écoulement, souvent sous la forme de tourbillons. À mesure que le nombre de Reynolds augmente, le nombre de tourbillons augmente et leur taille diminue : l'écoulement devient de plus en plus turbulent. L'analyse de ce type de transition, même si elle est délicate, reste possible.

En revanche, lorsque la transition est brusque, telle celle que l'on observe dans

les écoulements des canalisations, aucune analyse n'était jusqu'à présent possible. Dans un écoulement régulier, apparaissent soudainement de petites régions turbulentes, ou « spots », entourées d'un écoulement laminaire. Pour étudier cette transition, nous avons examiné un écoulement de cisaillement : dans une cuve remplie d'eau, une courroie en rotation entraîne l'eau dans deux sens opposés.

L'écoulement initial est laminaire. On le perturbe en injectant de l'eau de manière quasi instantanée par un petit trou. Selon le nombre de Reynolds et l'amplitude de la perturbation, trois cas



Olivier Dauchot, Françoise Davaud

À l'aide d'un laser vert, on éclaire des paillettes argentées, mélangées à un liquide placé dans un écoulement de cisaillement. Dans ce type d'écoulement, la transition entre un état laminaire (régulier) et un état turbulent (désordonné) est caractérisée par l'apparition soudaine d'une région turbulente, entourée par des régions laminaires. Dans le spot turbulent de quelques centimètres visible sur cette photographie, l'orientation des paillettes fluctue et celles-ci renvoient la lumière dans la direction d'observation, alors que dans les régions laminaires, les paillettes restent dans le sens du courant et elles ne sont pas visibles.

Marburg au Congo

Une épidémie de fièvre hémorragique mortelle frappe le Congo depuis mars. Le filovirus incriminé serait le virus de Marburg, qui a causé en 1967 la première épidémie. Les malades vivaient dans des mines désaffectées et insalubres où les rats pullulent (et les excréments de rongeurs sont un réservoir de filovirus). L'étude de ces mines permettra de comprendre quels sont les réservoirs, les vecteurs et les voies de contamination empruntés par ces virus redoutables.

Symbiose à trois

Les fourmis champignonnistes *Attini* d'Amérique du Sud cultivent, sur des végétaux mastiqués, des champignons dans les sous-sols de leur colonies. Ce champignon symbiotique qui fournit l'unique nourriture des fourmis, est souvent la cible d'un parasite (*Escovopsis*) ; or les cultures des fourmis sont épargnées. Comment ? Des biologistes



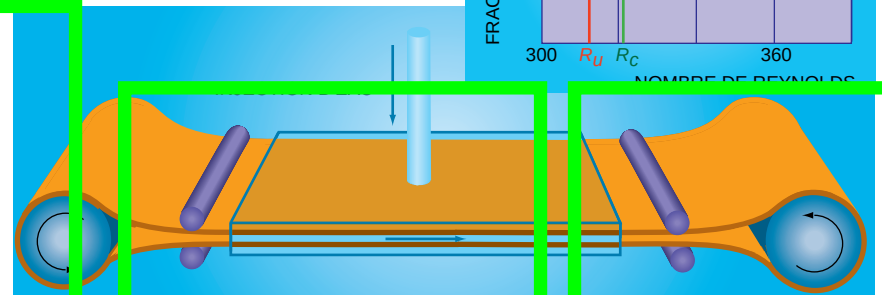
de l'Université de Toronto ont montré que les fourmis hébergeaient un second hôte, des bactéries fila-

reuses, *Streptomyces*. Présentes sur la carapace des fourmis, ces bactéries sécrètent un antibiotique fatal à *Escovopsis*. La lutte contre ces fourmis, fléau des cultures Sud-américaines, passera peut-être par l'élimination de leurs bactéries salvatrices.

Dyslexie et cervelet

La dyslexie, qui toucherait près de 20 pour cent de la population, est un trouble de l'acquisition de la lecture et de l'orthographe. Or les dyslexiques ont non seulement des difficultés à la lecture, mais aussi des difficultés de coordination et d'élocution. La dyslexie résulterait d'une anomalie de fonctionnement du cervelet, qui sert à l'acquisition des tâches automatiques. Une équipe de neurobiologistes a étudié l'activité de cette zone cérébrale chez six personnes dyslexiques et six personnes non dyslexiques, qui devaient répéter une séquence de mouvements des doigts : chez les premières, l'activité du cervelet n'a pas dépassé dix pour cent de l'activité du cervelet des personnes qui n'ont pas de difficultés de lecture.

Pour obtenir un écoulement laminaire, on entraîne de l'eau entre deux courroies en rotation. L'écoulement laminaire est perturbé par l'injection d'un jet d'eau. Des îlots de turbulence apparaissent dans l'écoulement laminaire, et la fraction turbulente augmente avec la vitesse de la courroie (déterminant le nombre de Reynolds).



apparaissent : soit la perturbation se résorbe et l'écoulement redevient laminaire, soit une région turbulente durable se forme, soit il apparaît une région turbulente qui dure assez longtemps avant de disparaître. Cette évolution du fluide est très sensible aux conditions de perturbation, et le comportement n'est pas déterministe : on ne connaît que la probabilité d'obtenir telle ou telle évolution en fonction de l'amplitude de la perturbation.

Pour des raisons pratiques, la transition inverse, de la turbulence au régime laminaire, est plus facile à observer. Partant d'un régime complètement turbulent, nous diminuons brusquement le nombre de Reynolds en réduisant la vitesse de la courroie. En étudiant l'évolution du système, on note une apparition et une disparition des régions turbulentes et des régions laminares, selon des règles strictes. Les domaines laminares ne redeviennent turbulents au contact d'un domaine turbulent : la turbulence se propage pour-

comme un feu de forêt. À l'inverse, au sein des domaines turbulents peuvent apparaître spontanément de nouveaux domaines laminares. Pour caractériser cette coexistence, nous mesurons la fraction turbulente de l'écoulement, c'est-à-dire le volume occupé par la turbulence dans l'écoulement. Cette grandeur change brusquement de valeur à la transition. La « intermittence spatio-temporelle » se maintient au-dessus d'un nombre de Reynolds critique R_c ; au-dessous du nombre de Reynolds critique, le régime devient totalement laminaire.

Le caractère discontinu de la transition s'interprète bien dans le cadre de la théorie des transitions de phase du type liquide-gaz. Nous espérons que cette analogie permettra de mieux comprendre la transition brusque vers la turbulence à l'aide de la théorie des transitions de phase.

Oliver DAUCHOT et François DAVIAUD, SPEC, CEA, Saclay

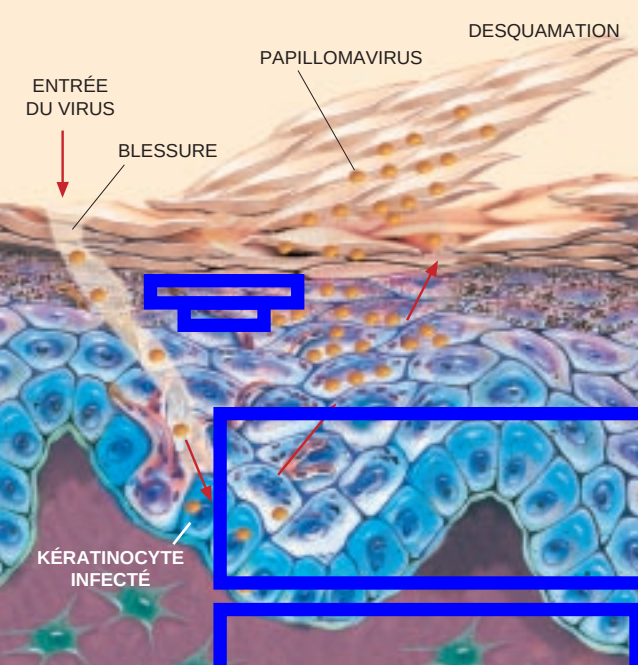
Les papillomavirus

Ces virus omniprésents se trouvent dans certaines lésions cutanées

Le premier membre de la famille des papillomavirus, responsable de verrues, a été découvert au début du xx^e siècle ; on a longtemps cru qu'il en était le seul représentant. Pourtant depuis quelques années, la famille s'est agrandie ; elle compte aujourd'hui plus de 100 membres. Pourquoi, chez certaines personnes, les lésions de la peau et des muqueuses que déclenchent divers types de papillomavirus disparaissent-elles rapidement ? Pourquoi perdurent-elles

chez d'autres ? Pourquoi, enfin, dégénèrent-elles en cancer chez quelques unes ? Les virologues sont face à des micro-organismes plutôt étranges, et voilà que la découverte de la localisation d'un gène de prédisposition aux papillomavirus et celle d'une de leurs « cachettes » ne font qu'ajouter au mystère. À moins que les pièces du puzzle se commencent au contraire à s'assembler.

Des études épidémiologiques avaient montré que la susceptibilité aux papillomavirus et les risques d'évolution des infections vers un cancer semblent dépendre du type de virus, de l'efficacité du système immunitaire et de facteurs génétiques de prédisposition. Gérard Orth, Michel Favre et Nicolas Ramoz, de l'Unité mixte des papillomavirus (Institut Pasteur-INSERM U190),



Les papillomavirus pénètrent dans l'épiderme par une petite lésion de la peau ou des muqueuses. Ils infectent les kératinocytes ; après s'être multipliés sous l'influence des virus, les kératinocytes migrent vers la surface, et le virus utilise la machinerie cellulaire pour se multiplier. Les couches superficielles de l'épiderme ou des muqueuses qui desquament sont riches en papillomavirus.

ont trouvé que les familles atteintes d'une maladie très rare, l'épidermodysplasie verruciforme, due à un groupe de papillomavirus, dont le PVH5, ont effectivement un gène de prédisposition à la maladie localisé sur le chromosome 17. L'épidermodysplasie verruciforme se manifeste dès l'enfance par des taches pigmentées et par des verrues cutanées, dont certaines dégénèrent en cancer, à l'âge adulte, quand elles sont associées au PVH5.

En collaboration avec l'équipe de Stefania Jablonska, à Varsovie, les virologues de l'Institut Pasteur ont également montré que la peau des personnes atteintes de psoriasis contient le papillomavirus PVH5! Cette affection dermatologique se manifeste par des plaques qui sont le siège d'une hyperprolifération de l'épiderme, de phénomènes inflammatoires et d'une desquamation intense. Les plaques blanches de kératinocytes (les principales cellules de l'épiderme) en cours de desquamation peuvent être localisées, par exemple sur les coudes, ou disséminées sur tout le corps.

G. Orlowski et ses collègues ont découvert des anticorps anti-PVH5 dans le sang de un à cinq pour cent de la population générale, mais chez 25 pour cent des personnes atteintes de psoriasis. En utilisant des méthodes d'amplification des gènes extrêmement sensibles, ils ont découvert de l'ADN de PVH5 dans 90 pour cent des lésions cutanées de personnes atteintes de psoriasis.

Pourquoi le virus est-il détecté si fréquemment dans les lésions de psoriasis? On l'ignore encore. Chez les malades atteints d'épidermodysplasie verruciforme,

some 1%, dans une région contenant un gène de prédisposition au psoriasis. Imaginons que ce soit le même gène et qu'il code une protéine de régulation qui, en se fixant sur l'ADN du virus, l'inactive. Chez les personnes où les papillomavirus de l'épidermodysplasie verruciforme sont infectifs, la protéine inhibitrice normale empêcherait ces virus d'infecter les cellules de l'épiderme. Au contraire, quand le gène de prédisposition produit une protéine anormale, le virus ne serait pas inactivé et les cellules cibles de la peau seraient infectées.

Selon l'hypothèse qui va être testée, le gène de prédisposition à l'épidermodysplasie verruciforme et le gène de prédisposition au psoriasis seraient un seul et même gène. Certaines mutations de ce gène favoriseraient la première maladie, dans laquelle le papillomavirus PVH5 est produit en grande quantité, d'autres la seconde, où la production virale est faible. Dans le cas de l'épidermodysplasie verruciforme, les cellules infectées produisent deux protéines virales redoutables, car elles inhibent des protéines de l'hôte qui contrôlent la division cellulaire et luttent contre les mécanismes de cancérogenèse. Quand ces protéines de protection sont inhibées, les remparts contre les mécanismes cancéreux s'effondrent.

Un fait semble désormais établi : le papillomavirus PVH5 se terre dans les couches profondes de l'épiderme des personnes atteintes de psoriasis, formant une sorte de «réservoir» du virus. Trouvera-t-on d'autres réservoirs aussi surprenants pour les autres papillomavirus?

le virus infecte les couches profondes de l'épiderme après avoir pénétré dans la peau par une petite lésion. Dans ces couches profondes, les cellules basales (des kératinocytes) se multiplient rapidement sous l'influence du virus, mais ce dernier ne se réplique pas pendant cette période. Quand elles

les basales se différencient et migrent vers la surface. C'est à ce moment que le virus détourne la machinerie cellulaire à son profit pour se répliquer en grande quantité. Chaque cellule migrant vers la surface y libère de nombreuses particules virales.

Avec les dermatologues Luis-Alfredo Rueda (Colombie) et Bakar Bouadjar (Algérie), les dermatologistes ont montré que le gène de prédisposition à l'épidermodysplasie verruciforme est localisé sur le chromo-

Un recrutement
sélectif,
une réelle formation
par la recherche,
conduisent,
en trois ans d'études au :

MAGISTÈRE DE PHYSIQUE

Ce diplôme universitaire de haut niveau
(Bac+5), préparant à la formation
fondamentale et appliquée,
recherche, prépare aussi bien à un
travail doctoral qu'à des emplois
en milieu industriel.

Pour tous renseignements,
s'adresser directement
à l'un des responsables :

MAGISTÈRE DE PHYSIQUE DE GRENOBLE

«Ph. recherche» et «Ph. applications»
Université Joseph Fourier
BP 517 - 38041 GRENOBLE cedex 9
Tél. 04 76 87 70 32/47 10 - Fax 04 76 86 30 00
lpuech@labs.polycnrs-gre.fr
http://www.physique.univ-gre.fr

MAGISTÈRE DE SCIENCES

DE LA MATIÈRE
Université Claude Bernard
et École Normale Supérieure de Lyon
Bât. 05 - 47, bd du 11 novembre 1918
69622 VILLEURBANNE cedex
Tél. 04 72 43 10 84 - Fax 04 72 43 15 07
vialle@hplasm2.univ-lyon1.fr

MAGISTÈRE INTERUNIVERSITAIRE

DE PHYSIQUE
Universités Paris 6, 7, 11, 13
et École Normale Supérieure
24, rue Lhomond - 75231 PARIS cedex 05
Tél. 01 44 32 76 61 - Fax 01 44 32 25 06
http://www.physique.univ-paris6.fr

MAGISTÈRE DE PHYSIQUE D'ORSAY

Université Paris Sud
Bât 400 - 91405 ORSAY
Tél. 01 69 15 74 55 - Fax 01 69 15 64 59
http://www.magistere.u-psud.fr/phys

MAGISTÈRE DE PHYSIQUE DE PARIS 7

Université Denis Diderot
Tour 63-34 - 4^e étage
2, place Jussieu - 75251 PARIS cedex 05
Tél. 01 44 27 51 12 - Fax 01 44 27 52 94
dherzog@ccr.jussieu.fr
http://www.sig7.jussieu.fr/UFRPHYSIQUE.htm

MAGISTÈRE MATÉRIAUX

Université de Rennes 1
Campus de Beaulieu - 35042 RENNES
cedex
Tél. 02 99 28 62 66/16 05 - Fax 02 99 38 34 87
Jean.Guyader@univ-rennes1.fr

MAGISTÈRE MULTIMATÉRIAUX DE STRUCTURE

Université de Haute-Alsace
Faculté des Sciences et Techniques (FST)
4, rue des Frères Lumière
68093 MULHOUSE cedex
Tél. 03 89 33 63 44/57 - Fax 03 89 33 60 83
direction.lpse@univ-mulhouse.fr

Une «perle de soufre»

Une bactérie visible à l'œil nu a été découverte. Elle pourrait dépolluer les eaux du littoral.

Imaginez un zoologiste à la recherche de nouvelles espèces de souris. Les plus grosses connues sont de la taille d'un gros rat, mais il en découvre une de la taille d'un minuscule éléphant. C'est ce qui est arrivé à Heide Schulz et ses collègues de l'Institut Max Planck de Brême : ils cherchent des bactéries capables de produire du soufre à partir des sulfures et en ont trouvé une d'un volume 100 fois supérieur à celui de la plus grosse connue. Cette bactérie baptisée *Thiomargarita namibiensis* («la perle de soufre de Namibie») est visible à l'œil nu.

Au large de la Namibie, à bord du navire *Peter Kottsov*, les microbiologistes ont recueilli des sédiments déposés par 100 mètres de fond en espérant découvrir des espèces capables d'oxyder les sulfures telles que *Thioploca* et *Beggiatoa*, présentes à large du Chili et du Pérou. Ces deux zones présentent les mêmes caractéristiques : un courant ascendant apporte des eaux riches en éléments nutritifs à la surface, où de nombreuses espèces de plancton prospèrent, puis meurent. Les restes sédimentent et sont dégradés par d'autres bactéries qui produisent du soufre d'hydrogène.

Des bactéries *Thioploca* et *Beggiatoa* ont bien été observées, mais elles cohabitent avec de petites espèces brillantes de 0,1 à 0,7 millimètre de diamètre, qui ont été identifiées comme des bactéries, malgré les réserves de la communauté scientifique, surprise par la taille.

Le cytoplasme de ces cellules, c'est-à-dire leur milieu intérieur, est confiné en une

minuscule poche autour d'un grand compartiment nommé vacuole, rempli de granules de soufre (voir la figure) brillants, qui donnent à la bactérie son aspect perlé.

Thiomargarita namibiensis exploite l'énergie libérée par une chaîne de réactions biochimiques où interviennent des sulfures et des nitrates. Ainsi, l'organisme oxyde les sulfures en soufre et transforme les nitrates en azote. Cependant, dans l'habitat de la bactérie, les premiers sont présents uniquement dans les sédiments (occasionnels), tandis que les seconds n'existent que dans l'eau.

Comment utiliser deux éléments qui ne coexistent pas au même endroit ? Les bactéries sud-américaines confrontées au même problème s'assemblent en petites chaquettes de quelques individus entourées par une gaine de mucus. Elles établissent ainsi un tunnel entre les milieux sulfuré et nitraté.

Thiomargarita namibiensis vit également en groupe (de 10 à 100 individus). Sa stratégie est néanmoins différente : elle profite des mouvements des sédiments remués par exemple lors des tempêtes, pour emmagasiner des nitrates dans sa vacuole dès qu'elle est au contact de l'eau.

Lorsque le temps se calme, elle retombe dans le sédiment où, à la manière d'un plongeur en apnée, elle utilise sa réserve jusqu'à la prochaine tempête.

Ce comportement explique sa taille : d'un point de vue évolutif, on croit que plus une bactérie est grosse, plus ses réserves sont importantes et plus longtemps elle peut attendre le prochain contact avec l'eau lors de la prochaine tempête.

Thiomargarita namibiensis, déjà utile pour le biotope marin, car elle dégrade les sulfures qui sont toxiques pour de nombreuses espèces, sera peut-être également utilisée par l'homme pour nettoyer les eaux côtières des nitrates issus des engrais déversés dans les champs et entraînés par les eaux de pluie jusqu'au littoral.

Enfin, les microbiologistes n'ont pas encore réussi à isoler la bactérie en culture. De plus, sa croissance est très lente : la population de *Thiomargarita namibiensis* double en une ou deux semaines, tandis qu'il suffit de 20 minutes à la bactérie *Escherichia coli*. Cet obstacle reste à lever.

Lorsque l'océan est calme, *Thiomargarita namibiensis* (au centre) reste dans le sédiment dont elle extrait les sulfures d'hydrogène (flèches vertes). Pendant les tempêtes, le sédiment est remué, la bactérie, au contact de l'eau emmagasine des nitrates (flèches jaunes) dans sa vacuole. Elle produit du soufre qui est stocké sous forme de petites billes d'aspect nacré et de l'azote qui est libéré.



Cartes d'extinction

L'extinction des étoiles révèle la masse des nuages moléculaires.

Les nuages de gaz froids et denses qui constituent près de dix pour cent de la masse de notre Galaxie sont essentiellement formés d'hydrogène. Grâce à un nouveau traitement des comptages d'étoiles, nous avons établi les cartes des nuages de gaz, révélant nombre de cœurs denses où se forment les étoiles.

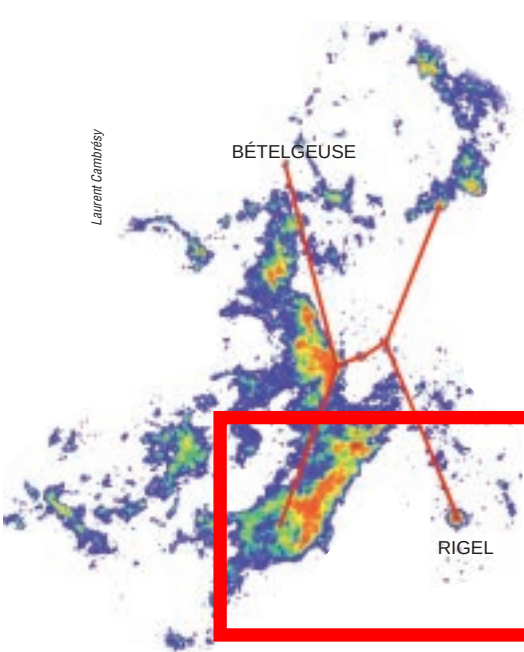
Parmi la Voie lactée, lorsque la Voie lactée déchire le ciel, on discerne des zones sombres où les étoiles semblent absentes. Le phénomène ne résulte pas d'un déficit d'étoiles dans cette région du ciel, mais de la présence de gigantesques nuages de gaz et de poussières interstellaires interceptés entre les étoiles et la Terre. Comment étudier ces nuages ? En comptant les étoiles. On connaît la répartition des étoiles en fonction de la région du ciel et on déduit la quantité de matière qui absorbe la lumière du quotient de la densité d'étoiles qui résulte du comptage et du densité théorique d'étoiles.

Cette approche, utilisée depuis 1923, était manuelle : jusqu'en 1996, on comptait le nombre d'étoiles dans chaque case d'une grille posée sur une plaque photographique. En remplaçant la grille de taille fixe par une grille informatique adaptative et en filtrant le bruit à l'aide d'une décomposition en ondelettes (une transformation mathématique adaptée au traitement des images sur plusieurs échelles spatiales), nous avons reconstruit la géométrie des nuages.

Grâce à la résolution des cartes, on mesure une extinction de l'ordre de cinq magnitudes (une extinction de une magnitude correspond à une luminosité 2,5 fois inférieure). Toutefois, cette extinction est en moyenne qui résulte de la résolution des comptages et on peut estimer que l'extinction est supérieure. Par exemple, dans le nuage d'Orion, on a calculé une extinction de 20 magnitudes visuelles, soit une absorption d'un facteur 100 millions.

À quoi cela correspond-il ? L'œil humain distingue les étoiles de magnitude inférieure à six (plus la magnitude est élevée, plus l'étoile est faible). Or, l'étoile la plus brillante du ciel, ayant une magnitude de $-1,6$, une extinction de 5 magnitudes suffit à la rendre invisible à l'œil nu ($-1,6 + 8 > 6$). En conséquence, si l'on plaçait Sirius derrière le nuage d'Orion, elle disparaîtrait de notre vue.

Lorsque l'on étudie des régions très absorbantes, l'extinction de la lumière visible ne suffit plus, car les étoiles du



Cette carte du nuage moléculaire d'Orion montre l'étendue du nuage par rapport à la constellation d'Orion, aisément identifiable sur le ciel. Les régions rouges sont celles où l'extinction des étoiles situées à l'arrière du nuage est la plus forte et donc où l'absorption de la matière est la plus grande. On estime que la masse du nuage est proche de 300 000 fois la masse du Soleil.

fond sont tellement absorbées qu'elles disparaissent. Aussi, complète-t-on ces observations avec des comptages dans l'infrarouge proche (longueurs d'onde de l'ordre du micromètre). Cette gamme de longueur d'onde est bien adaptée à l'observation de ces régions : moins sensible à l'extinction, elle permet de sonder les cœurs les plus denses des nuages.

L'un des objectifs du relevé DENIS est justement de cartographier tout le ciel austral dans l'infrarouge proche. Commencés en 1996, à l'observatoire de la Silla, au Chili, les observations de ce relevé ont déjà permis de cartographier le nuage du Caméléon. On a ainsi distingué une dizaine de cœurs denses, alors que les observations dans le visible n'en faisaient apparaître que quatre. Les données de DENIS sont également un remarquable outil de recherche d'étoiles jeunes, car celles-ci émettent la majeure partie de leur rayonnement dans l'infrarouge. Toujours dans le nuage du Caméléon, on a trouvé une cinquantaine de candidats étoiles jeunes (en plus des 130 connues auparavant dans ce nuage). Leur statut devra être confirmé par des observations

spectrales. Les comparaisons des cartes d'extinction avec les observations dans le domaine radio sont également fructueuses. Les différences entre les cartes d'émission du monoxyde de carbone (CO) et les cartes d'extinction révèlent les régions où le monoxyde de carbone est détruit par un fort rayonnement stellaire local. De même, la comparaison entre cartes d'extinction dans le proche infrarouge (ou dans le visible) et l'émission dans l'infrarouge lointain obtenue par les satellites IRAS et ISO indique la nature des grains du nuage : les variations du quotient extinction sur émission traduisent probablement des changements dans la composition chimique des grains de poussière.

L'utilisation systématique des comptages d'étoiles sera un outil précieux pour cartographier les nuages moléculaires proches. Ces cartes ont déjà révélé de nouveaux nuages, tel un énorme nuage d'une masse d'environ 10 000 masses solaires dans la constellation du Loup. Gageons que les données de DENIS, dont les observations continueront jusqu'en 2000, révéleront d'autres surprises.

Laurent CAMBRÉSY, Obs. de Meudon

Calcul verbal

Notre cerveau traite différemment calcul exact et calcul approché.

Les ordinateurs calculent par des méthodes différentes, et dans des zones différentes des microprocesseurs, avec des entiers ou avec des multiples de puissances de dix positives ou négatives (les nombres à virgule flottante). Les informaticiens ignoraient que leurs propres capacités de calcul suivent aussi deux chemins différents : lorsque nous souhaitons donner un résultat exact, nous utilisons des circuits neuronaux associés au langage, tandis que la production d'un résultat approximatif repose sur un «sens des nombres» de type analogique.

Des personnes atteintes de lésions cérébrales ne peuvent répondre à la question simple «neuf est-il plus proche de dix ou de cinq», bien qu'elles récitent sans problème des tables de multiplication. À l'opposé, des individus incapables d'additionner dix et deux savent tout de suite que le résultat est plus proche de trois que de neuf. Par ailleurs, des enfants de six mois, qui ne savent ni compter ni parler, manifestent un sens des quantités : ils sont surpris lorsque trois marionnettes passent derrière un rideau et quand il n'en reste qu'une une fois le rideau levé. Ces quelques

indices, parmi d'autres, incitent à penser que nous pouvons manipuler des nombres sans savoir compter, et que cette manipulation sollicite des capacités différentes de celles du calcul exact.

Pour tester ces hypothèses, Stanislas Dehaene et ses collègues du Centre hospitalier Frédéric Joliot d'Orsay et de l'Institut de technologie du Massachusetts ont entraîné des bilingues au calcul mental, dans l'une de leurs deux langues. Ils leur ont appris à choisir, entre deux solutions possibles, le résultat exact ou le plus proche d'une série d'additions en base dix, en base six ou en base huit, ou la valeur approchée du logarithme à base deux ou de la racine cubique de plusieurs nombres.

Premier résultat, encourageant pour les écoles, l'entraînement améliore les performances dans tous les exercices : le temps de réponse diminue. Cette amélioration est-elle transférable dans l'autre langue ? Pour le calcul exact, la réponse arrive toujours beaucoup plus vite dans la langue d'entraînement : on retrouve le fait, souvent rapporté, que les bilingues comptent préférentiellement dans la langue où ils ont d'abord appris à le faire. Pour les calculs approchés, en revanche, l'entraînement dans une seule langue réduit le temps moyen de réponse dans les deux langues.

On obtient le même résultat lorsque, plutôt que la langue, on change les nombres sur lesquels portent les opérations : pour les approximations, l'amélioration est

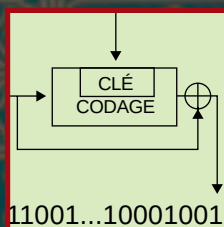
conservée mais pas pour le calcul exact. Le bénéfice de l'entraînement reposerait donc sur la mémorisation des résultats exacts, dans la langue où ils sont appris, tandis que, pour les approximations, le processus de réflexion lui-même semble accéléré.

L'observation, en imagerie par résonance magnétique, des zones du cerveau actives pendant les calculs et le suivi de cette activité en temps réel par électroencéphalographie (on détecte l'activité électrique à la surface du crâne) confirment que nous traitons très différemment les deux types de calculs. Notamment, le calcul exact active fortement, dans le lobe frontal inférieur gauche, une zone stimulée aussi par des exercices linguistiques, telles des associations sémantiques entre des mots. Nous utilisons dans ce cas les tables d'addition et de multiplication que nous avons apprises verbalement, et nous retenons sous la même forme les résultats des opérations : l'entraînement n'est pas facilement transférable à de nouveaux exercices (nous n'avons pas enregistré l'association nécessaire entre le problème et la solution), ni à une autre langue. En revanche, le calcul approché fait appel, dans les deux lobes pariétaux, à des zones actives aussi lorsque nous manipulons mentalement des objets, ou, plus étrangement lorsque nous bougeons les mains : ferions-nous inconsciemment des approximations sur nos doigts ?

La sécurité sur l'Internet



Pirates sur l'Internet
par Carolyn Wiener



Cryptographie et réseau
par Philip Zimmermann



Le paiement sur l'Internet
par Octavian Ureche et Réjean Plamondon

Pour la libéralisation de la cryptographie
par Ronald Rivest

En février 1998, des pirates informatiques s'introduisent, par le réseau Internet, dans plusieurs réseaux d'ordinateurs.

Ces intrusions semblent avoir été faites par deux adolescents de Californie qui cherchaient à accéder à des informations confidentielles sur les équipages, le personnel et les soldes des militaires (pendant un temps, le Pentagone a cru que ces attaques étaient commanditées par Saddam Hussein). Ces agressions électroniques ne sont pas rares : au cours de l'année 1998, deux tiers des entreprises surveillées par les services américains de contre-espionnage ont été victimes de violations informatiques.

Dans ce dossier, des experts décrivent les techniques mises en œuvre pour déjouer les manœuvres des indésirables, comment les « pare-feu informatiques » détectent et arrêtent les intrus ; si ces défenses cédaient, des techniques de cryptographie assureraient néanmoins le secret des données.

Ces techniques de cryptographie permettent aussi l'émission de messages secrets sur le réseau Internet ainsi que le paiement sécurisé. La sécurité informatique est un atout pour la préservation des richesses accessibles par le réseau Internet.

Pirates sur l'Internet

CAROLYN MEINEL

Les pirates informatiques emploient un arsenal varié pour commettre leurs méfaits. Pourtant, aucun d'eux n'est invincible.

La fiction présente des techniques et des logiciels réels. Certains des événements relatés ici sont issus de mes propres expériences. Je remercie le fournisseur d'accès Rt66 Internet qui a testé la plupart des logiciels décrits dans cet article.

La nuit est tombée depuis longtemps quand, face à son ordinateur, Jean Nau se connecte sur le réseau Internet à un «système de causerie» où chaque utilisateur introduit des remarques et lit celles des autres en temps réel. Dans la zone de dialogue consacrée au puissant système d'exploitation *Unix*, il observe les habitués : leurs contacts, leurs alliances, leurs échanges de connaissances. Ces échanges ressemblent à ceux qui avaient sans doute lieu dans les tavernes de l'île de la Tortue après un abordage réussi.

Imbu de ses compétences informatiques, Nau attend l'occasion – par exemple, une question naïve – de provoquer une bagarre verbale. Il saisit sa chance lorsqu'un certain Robert Surcouf demande si quelqu'un sait comment écrire un programme de commande d'une station météorologique personnelle. Nau répond «rtfm» (initiales de l'expression anglaise *read the fucking manual*, ce qui signifie : lis le p... de manuel).

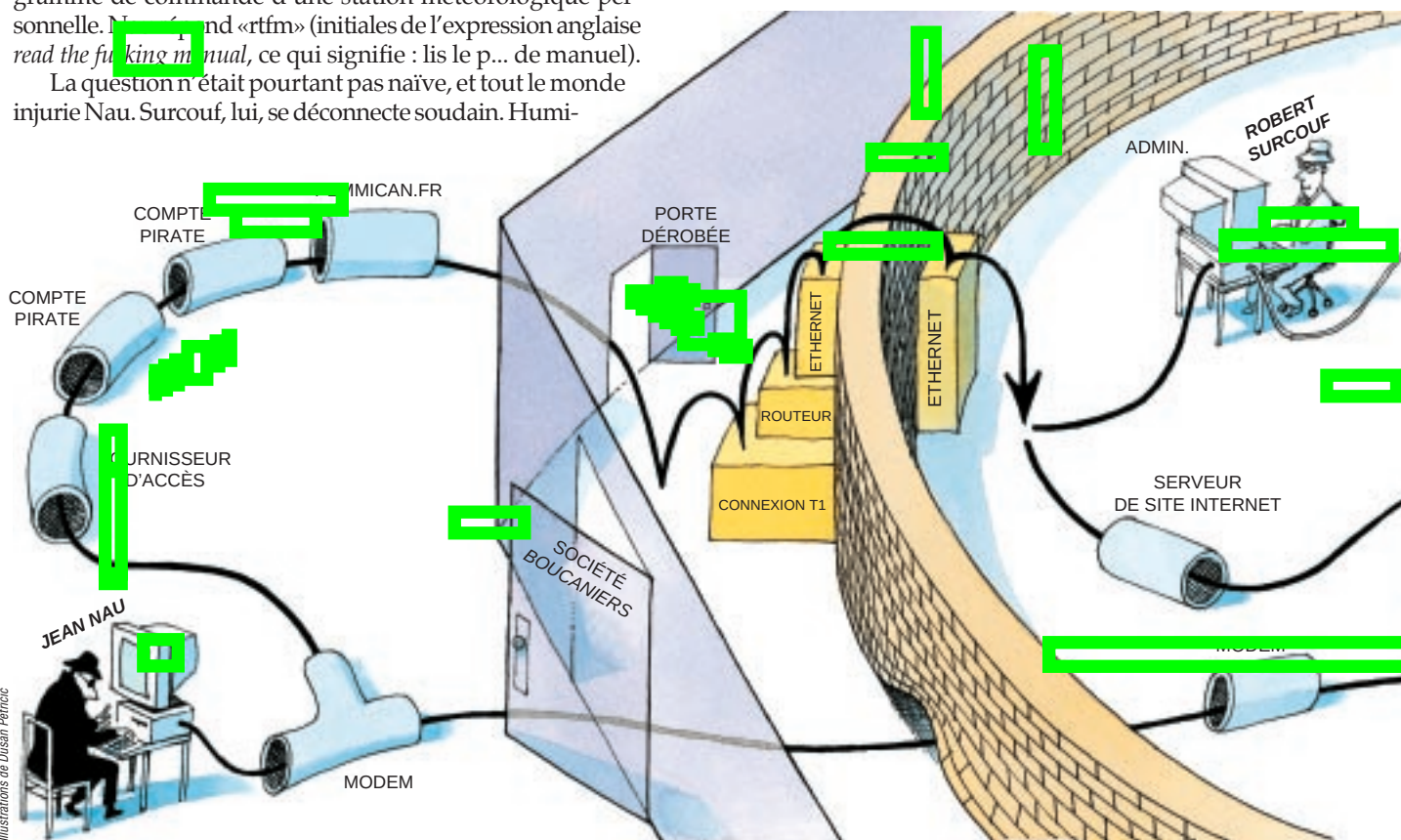
La question n'était pourtant pas naïve, et tout le monde injurie Nau. Surcouf, lui, se déconnecte soudain. Humi-

lié, Nau veut sa revanche. Il obtient rapidement l'adresse électronique `surcouf@boucanier.fr`, puis apprend que Surcouf est l'administrateur du réseau informatique `boucanier.fr`.

Grâce au logiciel *Strobe*, Nau essaie de se connecter à chacun des milliers de ports virtuels, c'est-à-dire des canaux de connexion, de `boucanier.fr`. Sur certains ports, un programme nommé *Démon* répond automatiquement. Découvrira-t-il une faille dans l'un d'eux ?

Tentative après tentative, le logiciel *Strobe* rencontre un mur, le «pare-feu» de Surcouf ; ce logiciel puissant lit l'entête de chaque message, par exemple une tentative du logiciel *Strobe*, et identifie sa destination. Le pare-feu rejette ou accepte les messages en fonction de règles d'accès définies. Face à *Strobe*, il réagit en envoyant des données dépourvues de sens, jusqu'à saturer l'ordinateur personnel de Nau. Parallèlement, un courrier électronique est envoyé au fournisseur d'accès Internet de Nau : quelques minutes plus tard, Nau, soupçonné d'infraction informatique, est privé d'accès au réseau.

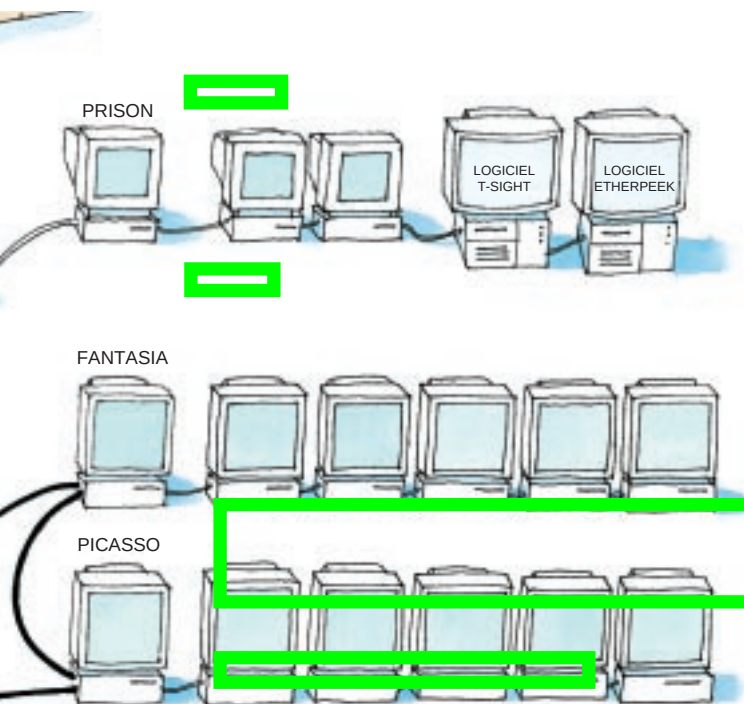
Illustrations de Dusan Petric



Malgré la rapidité des représailles, Nau n'est pas neutralisé : ce n'est que l'un de ses nombreux comptes piratés qui est clôturé. La fermeture de ce compte l'élimine de la causerie, où il apparaît comme un cuistre ou un lâche. Il est temps d'utiliser une autre arme : un scanner de ports furtif.

Ce programme est plus subtil que *Strobe*, car il manipule les informations échangées lors des communications entre les ordinateurs. Lorsqu'un ordinateur souhaite transmettre un message, il envoie tout d'abord un signal nommé SYN, destiné à la synchronisation des deux ordinateurs. Le programme qui le reçoit répond par un double signal (un d'accord, ACK, et un de synchronisation, SYN), et par une valeur de temporisation qui sera utilisée pour régler la transmission des données (voir la figure 4) et, en outre, ralentir le temps de réaction de l'ordinateur émetteur. Ce dernier envoie enfin un signal d'accord, ACK ; puis les salutations achevées, il transmet son message, qui se termine par un signal FIN. Le destinataire retourne alors un signal d'accord, pour indiquer qu'il a bien reçu le message.

Un scanner de ports furtif ne respecte pas ce protocole (voir la figure 2) : il envoie un signal FIN prématuré à plusieurs canaux de connexion de l'ordinateur récepteur. De ce fait, le programme récepteur n'envoie aucune réponse, mais il transmet sur chaque canal un signal RST pour demander de recommencer la procédure. Ce signal RST, contrairement aux signaux ACK et SYN est caractéristique de l'ordinateur qui l'envoie : il fournit des informations importantes à l'attaquant, telles le type d'ordinateur et les démons en service. Cependant, sans les triples salutations, il n'identifie aucune connexion et n'enregistre pas la transmission dans ses comptes rendus d'opérations. Le scanner de ports furtif sonde un ordinateur en toute discrétion.



1. MALGRÉ LES PUISSANTS LOGICIELS DE DÉFENSE, par exemple les pare-feu qui stoppent les intrus non autorisés, les systèmes informatiques connectés au réseau Internet ont presque toujours plusieurs points faibles que les pirates exploitent.

Sur un site du réseau Internet, Nau trouve un scanner de ports furtif performant écrit en langage C. Nau doit le compiler, c'est-à-dire le traduire dans le langage de son ordinateur. Cependant, chaque version d'*Unix* est unique, et Nau n'a jamais étudié la programmation. Il n'en a jamais eu besoin, car tous les logiciels qu'un pirate désire sont en libre-service gratuit sur le réseau Internet. Reste à savoir les télécharger.

Le pirate Surcouf a suivi un parcours différent. Un ami technicien lui a appris comment gérer un système informatique. Puis il s'est perfectionné en affrontant son ami dans des jeux d'attaque et de défense de systèmes informatiques. Ils ont ensuite aidé le fournisseur d'accès Internet à renforcer sa propre sécurité. Surcouf a alors été embauché à temps partiel, en parallèle avec des études d'informatique.

Nau le pirate a donc commis sa première erreur : attaquer Surcouf, corsaire confirmé.

Le repérage des lieux

Au petit matin, Nau a traduit le programme. En quelques minutes, le scanner de ports furtifs lui fournit la liste des services proposés par boucanier.fr à des personnes dûment repériorisées. Un programme assurant la sécurité de l'interpréteur des commandes – pour qu'elles soient exécutables – grâce à des connexions codées et un serveur de site Internet retiennent son attention. Le cœur de Nau s'accélère. Un canal de connexion s'est entrouvert au moment de son examen. Un autre intrus l'a-t-il précédé ? A-t-il maintenant une porte dérobée pour pénétrer dans le système ?

La sonnerie d'un messenger de poche réveille Surcouf. Un programme de détection nommé *Etherpeek*, installé sur le réseau d'ordinateurs boucanier.fr, a décelé l'examen des canaux de connexion par Nau. Surcouf se précipite au bureau et, assis devant sa station de travail (un ordinateur performant), il fait le guet. Installés uniquement sur son propre ordinateur, ses meilleurs programmes de défense ne fonctionnent que lorsqu'il est aux commandes, afin d'éviter tout assaut de l'extérieur. Cependant, Surcouf n'observe aucune manœuvre : malgré la tentation, Nau, guidé par son intuition de pirate, a abandonné l'assaut.

Tout de même intrigué, Surcouf analyse les comptes rendus d'opérations de son ordinateur et retrouve l'adresse du message pirate. Par courrier électronique, il informe le fournisseur d'accès de Nau de la tentative d'effraction et lui demande des informations sur le compte du pirate. La clause de confidentialité des clients empêche la requête d'aboutir.

Toutefois, trois soirs plus tard, Nau découvre que son mot de passe n'est plus valable : son fournisseur d'accès lui apprend que son compte a été supprimé parce qu'il a utilisé un scanner de ports furtif.

Plus déterminé que jamais, Nau revient quelques minutes plus tard sur le réseau Internet grâce à un téléphone et à une carte bancaire. Il doit être prudent. De ce nouveau compte, il se connecte sur un de ses comptes piratés chez un autre fournisseur d'accès, et il apprend que le site informatique boucanier.fr appartient à la Société *Boucaniers*, qui produit de la viande fumée.

Nau tente alors de se connecter au réseau boucanier.fr par le canal inhabituel repéré trois nuits plus tôt. La réponse

est cinglant : «Espèce de marin d'eau douce! Peux-tu vraiment trouver un passage secret?» Puis le programme associé au canal transmet des données incohérentes et envoie un courrier électronique au système administrateur du fournisseur d'accès dénonçant la tentative de piratage. Quelques minutes plus tard, la connexion de Nau est supprimée.

Mieux vaut contourner le pare-feu sur la pointe des pieds plutôt que de le passer en force. D'un autre compte, également piraté, Nau tente, par une simple commande saisie sur le clavier, de dresser la liste des ordinateurs du réseau boucanier.fr.

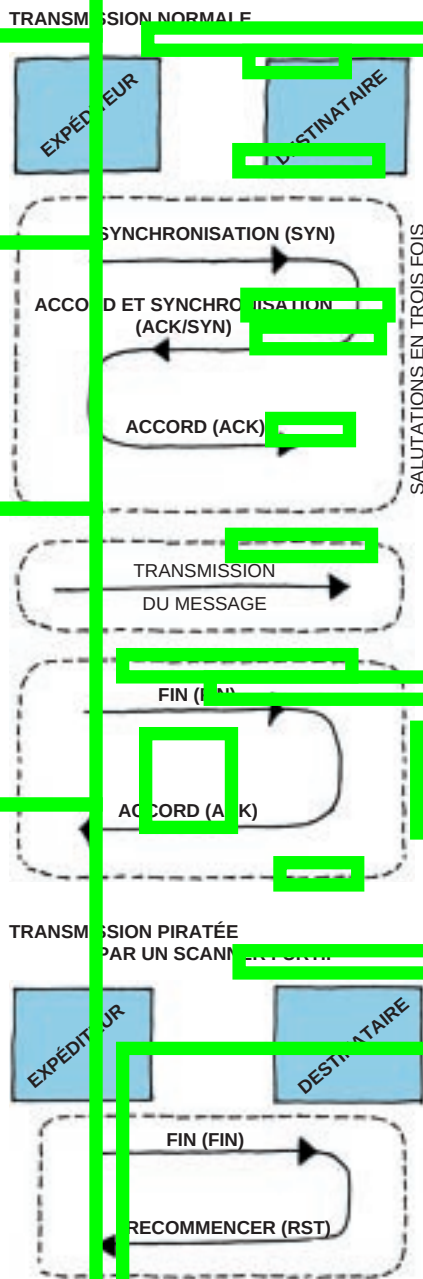
La commande ne fournit aucun résultat utilisable : Surcouf a probablement configuré le réseau de sorte que les données adressées à n'importe quel ordinateur transitent d'abord par un programme central, qui les redistribue ensuite. Cette méthode empêche les intrus d'accéder à l'intérieur du pare-feu.

Après avoir converti l'adresse informatique boucanier.fr en un nombre, Nau utilise un scanner d'adresses informatiques, puis il teste les 50 adresses numériques immédiatement inférieures et supérieures. Peut-être appartiennent-elles à des ordinateurs du réseau boucanier.fr, car les adresses numériques des ordinateurs d'un réseau sont souvent proches? Hélas, non.

Avec une autre commande, il découvre alors un second réseau appartenant à la Société Boucaniers : boucanum.fr, dont l'adresse numérique est éloignée de celle de boucanier.fr. Le scanner d'adresses découvre alors cinq ordinateurs dont l'adresse est numériquement proche de celle du réseau boucanum.fr.

Par précaution, Nau se connecte de son compte piraté à un autre compte piraté et, de là, vers un autre compte, d'où il exécute d'autres scanners de ports furtifs. Ces étapes supplémentaires engendreront toute procédure judiciaire, puisque celle-ci nécessiterait trois mandats de perquisition. Échaudé, il utilise également un programme nommé *Root kit*, grâce auquel il efface toute trace de son activité dans les comptes rendus utilisés pour détecter les activités furtives et les modifications des fichiers de configuration de cet ordinateur.

De son galion, Nau examine les ordinateurs de boucanier.fr et de boucanum.fr connectés au réseau Internet. Le scanner de ports furtif se glisse au



2. LES TRANSMISSIONS DE MESSAGES obéissent à un protocole rigide. L'expéditeur envoie un signal de synchronisation (SYN) des communications à venir (*en haut*). Le destinataire retourne alors un double signal (ACK/SYN) d'accord et de synchronisation pour accepter la demande. Enfin, l'expéditeur envoie à son tour un signal d'accord (ACK). Le message lui-même est alors transmis. Un signal de fin (FIN) le suit de peu. Le destinataire répond par un autre signal d'accord qui clôt définitivement la correspondance. Un pirate corrompt cet échange (*en bas*) en envoyant immédiatement un signal FIN auquel le destinataire est obligé de répondre par un signal pour recommencer (RST). La réponse – ou l'absence de réponse – fournit des informations sur le destinataire. Cependant, l'absence des triples salutations empêche la transmission d'être enregistrée dans les comptes rendus du destinataire. Le pirate sonde ainsi un ordinateur avec une certaine discrétion.

traverse un pare-feu vers chacun d'eux. Cependant, la manœuvre a été détectée par le programme *Etherpeek*, qui prévient le nouveau Surcouf.

Celui-ci déboule dans son bureau ; il identifie rapidement l'origine du scanner et alerte l'administratrice du système du troisième compte de Nau. Cependant, le programme *Root kit* dissimule Nau, qui continue avec impudence, grâce au scanner furtif et au logiciel *Strobe*, de chercher une adresse informatique non protégée par le pare-feu. Celui-ci ne fait que lui transmettre un flot de données incohérentes.

Cet afflux soudain convainc l'administratrice du compte de Nau qu'un agresseur est à l'œuvre. Elle déconnecte alors tout le système du réseau : la connexion de Nau s'arrête dans un sifflement.

À la recherche d'horaires décalés

Nau suppose alors que de nombreuses stations de travail non connectées au réseau boucanier.fr sont utilisées par des employés de la Société Boucaniers pour travailler chez eux. Ces ordinateurs, reliés directement, ne sont pas protégés par le pare-feu. La probabilité est grande, avec un modem, n'importe qui peut relier un ordinateur personnel à une ligne téléphonique.

Grâce à un logiciel de numérotation téléphonique automatique nommé *Shokdial*, Nau appelle chacune des lignes téléphoniques de la Société Boucaniers. Au siège de la société, les gardiens de nuit entendent sonner successivement les postes sans comprendre de quoi il retourne.

À 2 heures 57, un modem répond au programme *Shokdial* : Nau est alors face à une station de travail de la marque *Silicon Graphics* : «Boucaniers SA. Département informatique. Irix 6.3» (*Irix* est une forme de *Unix*). Nau a enfin trouvé une porte d'accès au fief de Surcouf.

Assez d'élégance ; Nau décide d'utiliser la porte. Il exécute un programme qui se connecte autant de fois que nécessaire pour découvrir le mot de passe d'un compte administrateur, c'est-à-dire un accès sans restrictions dans ses possibilités d'action, auquel il pourra agir en toute liberté. Le possesseur de cet ordinateur *Irix* aura peut-être autorisé la connexion à distance sur le compte administrateur.

La recherche de mot de passe commence avec les mots et les noms courants,

puis le programme teste des groupes de signes moins naturels : l'exploration peut durer des mois, voire des années. Cependant Nau est chanceux. Vers 5 heures, le prénom « Nancy » est identifié : le compte administrateur est accessible !

Nau est ravi. Il crée une fenêtre de dialogue entre lui et le système d'exploitation de l'ordinateur, d'où il dispose des mêmes pouvoirs que l'administrateur. Puis il renforce sa position en transférant un programme *Root kit* pour la discrétion et un programme *Sniffer* sur l'ordinateur de sa nouvelle victime. *Sniffer* intercepte et enregistre tout ce qui est enregistré par le programme *Sniffer* dans un fichier dissimulé. Le programme *Root kit* permet également de créer un chemin d'accès supplémentaire que Nau baptise « revanche » : mot de passe « MoRtSurCf ».

Nau termine sa nuit en déterminant que le compte administrateur auquel il a accédé est connecté sur l'ordinateur picasso du réseau boucanum.fr. Grâce au programme *Root kit*, l'utilisateur normal de l'ordinateur picasso ne remarquera pas que son ordinateur est maintenant commandé par quelqu'un d'autre. Surcouf ne détecte qu'une tentative d'intrusion dans boucanum.fr à partir du réseau boucanum.fr. Mais, faute d'informations suffisantes, il ne peut rien faire.

Deux jours plus tard, Nau revient à la charge. Il examine les comptes rendus du programme *Sniffer*. Toutes les informations concernant le trafic interne du réseau sont codées, mais le programme *Sniffer* a enregistré la connexion de quelqu'un, de l'ordinateur picasso sur un autre ordinateur du nom de fantasia.

Les pare-feu

Aucun réseau informatique relié au réseau Internet n'est invulnérable, mais des protections peuvent être installées. La première ligne de défense est le pare-feu, dont les deux types les plus fréquemment utilisés agissent soit au niveau des messages transmis, soit au niveau des logiciels. Le premier fonctionne sur une machine nommée routeur. Il examine dans chaque message entrant ou sortant les adresses de la source et de la destination, qu'il compare à des règles d'accès. Les messages autorisés sont transmis, les autres sont bloqués. Le second examine les adresses et le contenu des messages. Plus lent qu'un filtre de messages, il permet toutefois une politique de sécurité plus raffinée.

L'illustration représente un réseau informatique d'entreprise protégé par des pare-feu. Les lignes vertes symbolisent les messages autorisés, et les rouges les messages potentiellement suspects.

À l'extérieur du pare-feu (en orange), l'entreprise possède un réseau accessible au public, qui permet aux clients d'envoyer des courriers électroniques vers l'entreprise ou de naviguer sur ses différents sites informatiques. Cette zone (A) est analogue à l'espace d'accueil réservé au public que l'on trouve à l'entrée de certains établissements : aucune information confidentielle n'y est présente.

Un pare-feu fonctionnant au niveau des logiciels ressemble aux salles de police des aéroports (B) : les courriers électroniques sont inspectés. Les programmes reçus par le réseau Internet, qui peuvent contenir des instructions néfastes, sont envoyés sur un serveur mandataire, puis à un programme mandataire qui fonctionne en toute sécurité sur le réseau. Un programme mandataire est l'analogue du factotum (personnage en bleu) qui reçoit des messages de l'extérieur et les délivre au personnel.

Les pare-feu ne sont pas invincibles, ils peuvent être contournés (C) grâce à un modem téléphonique, à des disquettes ou à des bandes magnétiques volées, contenant des données confidentielles. Lorsque l'entreprise s'agrandit, des pare-feu supplémentaires sont nécessaires pour protéger les systèmes informatiques de

services importants, tel celui de la comptabilité.

Ces protections ressemblent à la porte d'acier d'une chambre forte (D) ; elles défendent les systèmes vitaux contre des attaques de l'intérieur ou de partenaires.

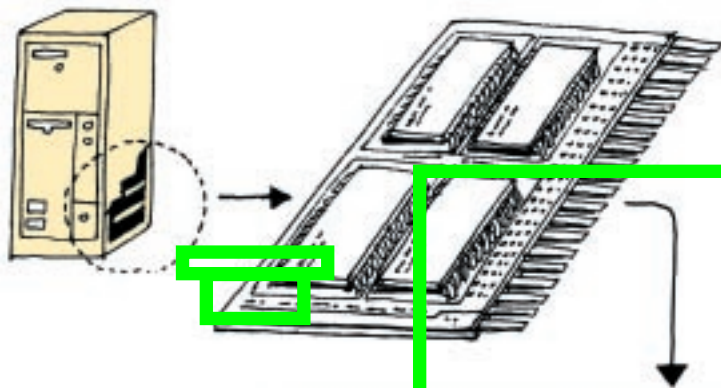
Un pare-feu fonctionnant au niveau des messages possède un peu la même fonction que les gardes de certaines entreprises (personnages en bleu). Selon la politique de sécurité de l'établissement, le filtre peut n'autoriser que l'entrée de messages provenant de certaines adresses, par exemple celles des partenaires d'affaires ou celles des fournisseurs. Les contrefaçons d'adresses sont évitées par une authentification codée, analogue à un badge de sécurité, qui assure que le fichier ou le programme entrant provient bien d'une adresse d'un partenaire de confiance.

William CHESWICK, Laboratoires Bell
Steven BELLOVIN, AT&T Research



ORDINATEUR
VICTIME

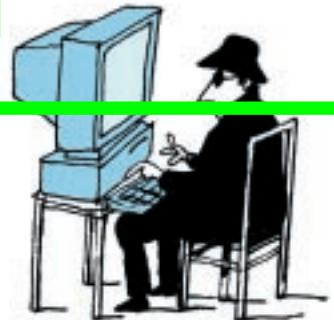
MÉMOIRE
VIVE



3. LE DÉLESTAGE D'UN FICHIER «CORE» est une opération que les pirates utilisent pour obtenir des informations secrètes. Après une erreur, l'ordinateur libère le contenu d'une partie de sa mémoire vive dans un fichier. Un pirate peut provoquer un tel incident et accéder ainsi à des informations importantes, tels des mots de passe.

FICHIER CACHÉ
DES MOTS
DE PASSE

```
root:I4.yoNjA4co5.:10386:-----1
diag:qiy2qsTuL1goU:10386:-----1
bin:AT1.Y7fcTCjxA:10386:-----1
personne:vt233NHYFD4:10386:-----1
rastrowDUF2ZhmTfjAo:10386:-----1
gitane:B6YO/a9yvUs3:10390:-----1
hdupont:ABDNGKodwomIE:10392:-----1
```



Nau passe maintenant à l'abordage d'une nouvelle zone du réseau.

Cet ordinateur fantasia est une station de travail de type SPARC, utilisée pour la création d'animations en images de synthèse, peut-être des génériques pour la télévision. C'est certainement un serveur auquel accèdent de nombreux autres ordinateurs. Nau cherche un fichier de mots de passe. Peut-être en trouvera-t-il certains valables sur d'autres ordinateurs à l'intérieur du réseau de la société.

Il localise ce fichier, mais n'y trouve que des «x»: l'information est probablement dissimulée ailleurs. Peu importe: utilisant le protocole de transfert de fichiers, Nau provoque une erreur qui oblige fantasia à transférer une partie de sa mémoire vive dans le compte que Nau s'est créé. Cette procédure est un «délestage de fichier core» (voir la figure 3), qui permet normalement aux programmeurs de découvrir des indices lors d'une panne de programme. Les mots de passe codés sont parfois stockés dans la mémoire vive. Lors d'une connexion, l'ordinateur code le mot de passe saisi par l'utilisateur et le compare aux

temporaires, nommé tampon. Les informations en excès dépassant la capacité du tampon et s'écoulent dans d'autres zones de la mémoire de l'ordinateur. Nau utilise ces dépassements de capacité (voir la figure 5) pour introduire dans la station de travail SPARC un programme grâce auquel il peut exécuter d'autres commandes et d'autres programmes. Ravi de son dernier forfait, Nau installe un autre programme Sniffer et un autre Root kit. Ce dernier ne masquera son œuvre qu'une fois activé; le forban efface donc les traces de ses premières activités.

Une dernière chose à faire encore. Quelqu'un est-il autorisé à se connecter sur fantasia à partir du réseau Internet? D'une simple commande qui affiche l'enregistrement de toutes les connexions sur fantasia, Nau constate que des utilisateurs prénommés nancy et vangogh sont récemment entrés sur fantasia par le réseau à partir du site pemmican.fr, qui se situe en dehors du pare-feu de la Société Boucaniers. Au moins Nau s'effondre, terrassé par le sommeil, mais satisfait: bientôt, il vaincra la Société Boucaniers.

La mise à mort

Le lendemain soir, Nau se présente sous une fausse adresse informatique chez pemmican.fr. Puis, en testant des signaux de synchronisation sur pemmican.fr, il détermine la valeur de temporisation qu'utilise pemmican.fr et falsifie sa propre origine. Il installe alors un programme Sniffer sur pemmican.fr et un interpréteur sécurisé pour se connecter en toute sécurité sur fantasia. Une commande lui fournit la liste des connexions actives à l'intérieur du réseau de la Société Boucaniers, où il découvre un nouvel ordinateur: «admin.boucanier.fr». L'ordinateur de Surcouf?

Parallèlement, Nau essaie chaque nouveau mot de passe et le nom d'utilisateur associé, découverts par son programme de recherche sur les ordinateurs du site boucanier.fr. Hélas, aucun ne fonctionne ailleurs que sur fantasia, qu'il a déjà conquis.

mots de passe déjà codés du fichier caché. Lorsque les deux coïncident, la connexion est autorisée. Grâce au délestage, Nau récupère le fichier de mots de passe codés. Il lance son programme de recherche de mots de passe: il va falloir patienter...

Impatient, Nau élabore déjà sa prochaine manœuvre. Avec un système d'exploitation Unix, lorsqu'un programme fournit trop de données à un espace de mémoire



Cependant, cette déconvenue est largement compensée par fantasma, qui lui fournit l'enregistrement de ce qu'a tapé l'utilisateur lorsqu'il a mis à jour la page Internet de la société. Nau y trouve le mot de passe nécessaire au piratage de la page Internet de Surcouf. Par ailleurs, son programme Sniffer installé sur l'ordinateur picasso lui indique qu'une certaine Nancy a utilisé cet ordinateur pour se connecter par une porte dérobée sur le compte administrateur d'admin.boucanier.fr,

dissimulée derrière un programme Root kit.

Il se glisse juste derrière elle et essaie de se connecter sur tous les ordinateurs de boucanier.fr. Hélas, Surcouf a été prudent : sur le réseau boucanier.fr, même les pouvoirs d'administrateur (administrateur) ne permettent pas d'accéder à d'autres ordinateurs sans nouveaux mots de passe. Nau est bloqué. Il retourne à l'assaut du site Internet. De son propre ordinateur, il installe une nouvelle version du site spécialement préparée.

La quarantaine de Java

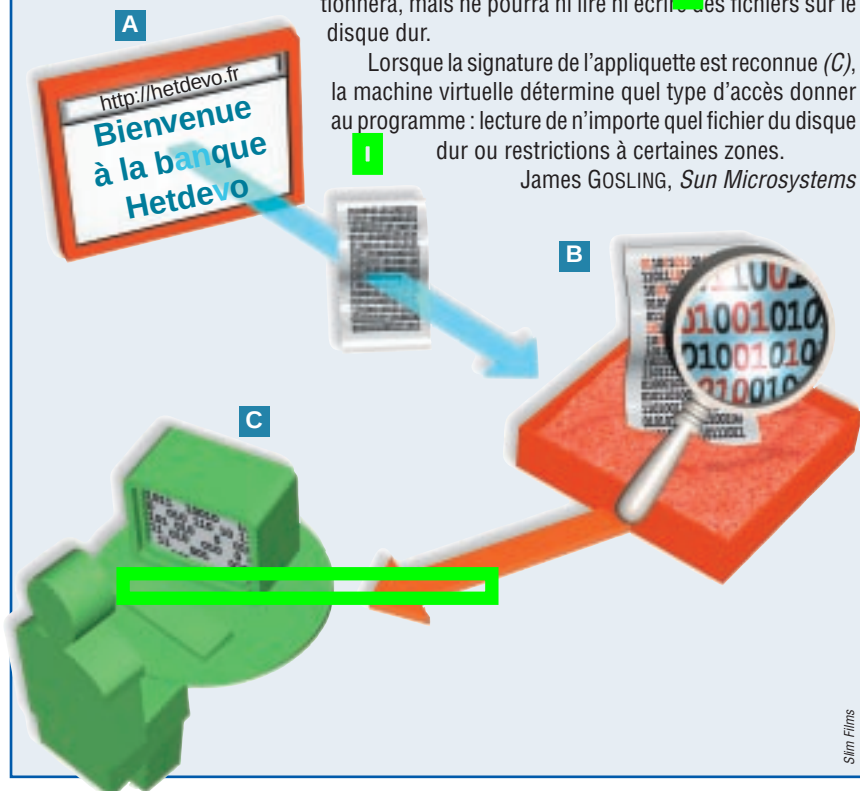
Le langage Java est utilisé par les programmeurs pour écrire de petits programmes, ou applications, qui peuvent être récupérés sur le réseau Internet ou sur d'autres réseaux d'ordinateurs. Un individu peut toutefois créer une applique malveillante qui efface des fichiers, vole des données ou injecte un virus. Cependant, le langage Java a prévu une sécurité : il s'agit d'un ensemble de logiciels, nommé machine virtuelle Java, indispensable à l'exécution de n'importe quelle applique.

Lorsqu'un utilisateur récupère une applique (A), par exemple un programme de gestion bancaire, la machine virtuelle empêche l'accès au disque dur, au réseau et à d'autres ressources vitales. L'applique se trouve alors en une sorte de quarantaine, d'où elle ne peut provoquer aucun dommage. L'applique n'est libérée que lorsque la machine virtuelle a vérifié qu'elle provient d'un source de confiance.

En premier lieu, un vérificateur de code détermine si l'applique est écrite dans une syntaxe Java correcte (B). Quand ce n'est pas le cas, le programme ne pourra pas être utilisé. Ensuite, la machine virtuelle recherche une signature numérique associée à l'applique qui identifie la personne ou l'organisme créateur et révèle toute altération. En cas de signature invérifiable, l'applique restera en quarantaine. Le programme fonctionnera, mais ne pourra ni lire ni écrire des fichiers sur le disque dur.

Lorsque la signature de l'applique est reconnue (C), la machine virtuelle détermine quel type d'accès donner au programme : lecture de n'importe quel fichier du disque dur ou restrictions à certaines zones.

James GOSLING, Sun Microsystems



Aujourd'hui, Surcouf travaille tard, il étudie les comptes rendus où apparaît un nombre inhabituel de connexions par le système commercial. Que s'est-il passé? L'aide de l'administratrice du système de pemmican.fr, une collègue qui lui est redevable, l'aidera sûrement.

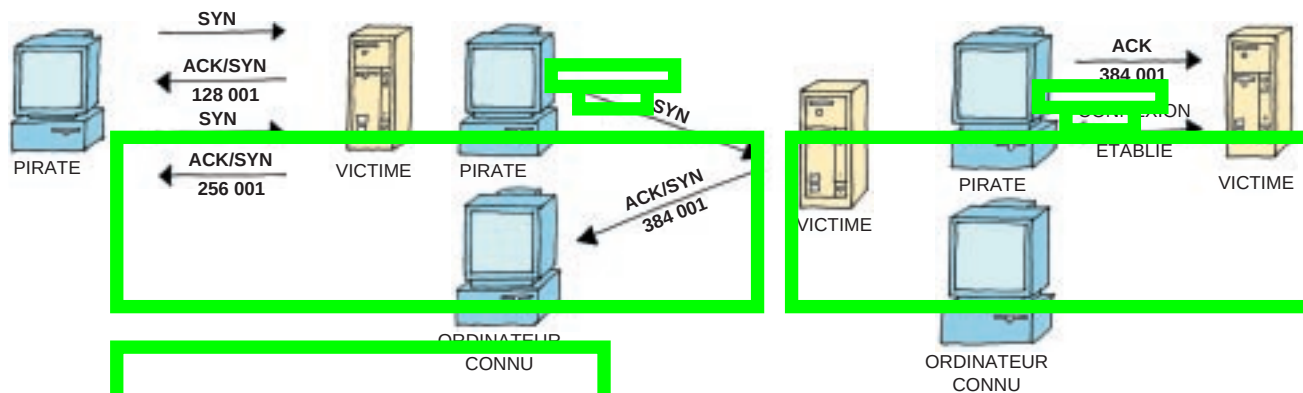
La sonnerie du téléphone retient Surcouf au moment de partir. Un client se plaint de la séquence pornographique affichée sur le site Internet de la Société *Boucaniers*. Après vérification, Surcouf débranche simplement le câble Ethernet, le cordon ombilical qui relie la société au réseau Internet.

Nau envisage de voir son mer-d'œuvre d'obscénité détruit aussi vite. Il s'inquiète également d'avoir laissé autant de traces derrière lui : il se connecte par modem sur l'ordinateur pommican, un accès qu'ignore Surcouf – et reformate complètement le disque dur de l'ordinateur d'administration du système. Le système de la société est

hors service. Surcouf ne rassemblera aucun indice. Surcouf redemarrera rapidement l'ordinateur d'administration, mais c'est trop tard : il devra complètement réinstaller les logiciels. Cependant, Nau ignore qu'un programme de détection *Etherpeek*, installé sur un des ordinateurs du réseau, a enregistré ses activités...

Nau est irrité : il noie boucanier.fr sous un flot de données. Peu après, Surcouf reçoit la plainte d'une représentante de la société qui n'arrive pas à se connecter sur le serveur de courrier électronique.

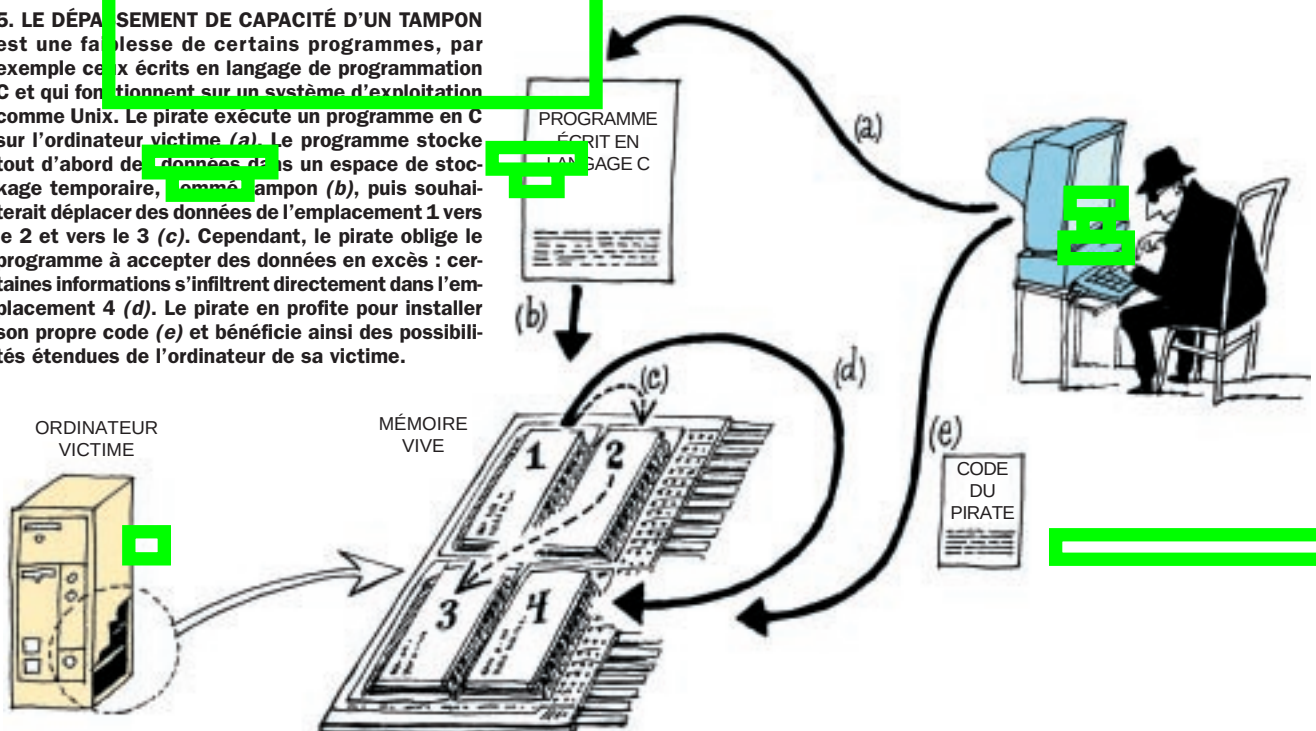
Le lendemain, Surcouf, exténué, demande au directeur technique de la Société *Boucaniers* l'autorisation d'effacer complètement tous les ordinateurs du réseau et de changer les mots de passe. Cependant, une telle mesure, bien que prudente, nécessiterait l'arrêt du système pour plusieurs jours. Le directeur refuse.

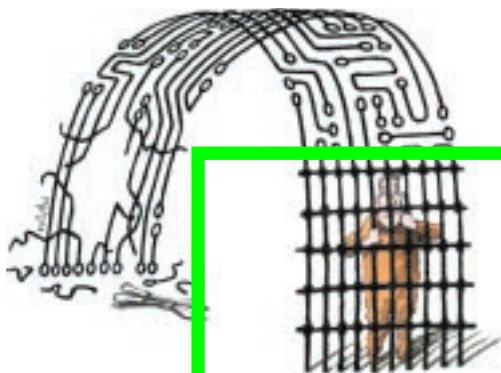


4. UNE ESCROQUERIE INTERNET permet au pirate de falsifier son identité. Il teste d'abord sa victime en lui envoyant de multiples signaux de synchronisation (SYN) pour obtenir, en réponse, un double signal d'accord et de synchronisation (ACK/SYN), et une valeur de temporisation (à gauche) caractéristique d'un système d'exploitation. Cette valeur augmente ici de 128 000 à chaque échange. Le pirate envoie ensuite de nombreux signaux de syn-

chronisation dont un est identique à celui d'un ordinateur connu de la victime, qui transmet alors un double signal d'accord et de synchronisation à cet ordinateur autorisé (au centre). Le pirate ne reçoit pas cette réponse, mais poursuit la correspondance. Il envoie un signal d'accord avec la valeur de temporisation correcte : la communication entre son ordinateur et sa victime est établie (à droite). Le piratage commence

5. LE DÉPASSEMENT DE CAPACITÉ D'UN TAMPON est une faiblesse de certains programmes, par exemple ceux écrits en langage de programmation C et qui fonctionnent sur un système d'exploitation comme Unix. Le pirate exécute un programme en C sur l'ordinateur victime (a). Le programme stocke tout d'abord des données dans un espace de stockage temporaire, nommé tampon (b), puis souhaiterait déplacer des données de l'emplacement 1 vers le 2 et vers le 3 (c). Cependant, le pirate oblige le programme à accepter des données en excès : certaines informations s'infiltreront directement dans l'emplacement 4 (d). Le pirate en profite pour installer son propre code (e) et bénéficie ainsi des possibilités étendues de l'ordinateur de sa victime.





Nau a franchi depuis longtemps la frontière légale du piratage. Néanmoins, la Direction de la surveillance du territoire, occupée par plusieurs affaires de piratage de réseaux d'ordinateurs des facultés et des grandes écoles ne peut aider Surcouf. Il doit rassembler seul les preuves.

Puisque le forban est resté connecté alors que le système n'était plus relié physiquement au réseau de l'Internet, Surcouf soupçonne l'existence d'un modem piraté dans les bureaux. Son propre numéroteur téléphonique automatique découvre bientôt la brèche utilisée par Nau.

Il réinstalle alors sur son ordinateur d'administration un système propre, puis met en place un logiciel antipirates, nommé *T-Sight*, qui contrôle tous les ordinateurs du réseau de la société. Surcouf prépare également un piège : le logiciel *T-Sight* guettera la prochaine connexion sur admin.boucanier.fr et dirigera l'intrus sur un ordinateur « prison » où le coupable sera maîtrisé et identifié. Surcouf, avec une équipe de programmeurs, camoufle sa prison en un système multi-utilisateurs et y place des données financières factices en guise d'appât.

Le comble de l'orgueil

Deux jours plus tard, à 20 heures 17, quelqu'un s'introduit dans l'ordinateur admin.boucanier.fr. C'est Nau ! Pourquoi est-il revenu si tôt ? Nau a beaucoup apprécié – il en a même ri aux larmes – que les pirates de l'informatique et les chaînes de télévision parlaient de ses talents. Il se sent invincible. Erreur...

Trop pressé, il se connecte sans les précautions habituelles sur pemmican.fr, puis sur l'ordinateur fantasia. Appâté par le leurre, il se dirige rapidement vers la prison. Au comble de

l'excitation, il examine ce qu'il croit être des données financières importantes.

De son côté, Surcouf analyse rapidement les informations fournies par le programme *T-Sight* et obtient le mot de passe que Nau utilise pour pirater fantasia. Il suit ainsi l'intrus jusqu'à pemmican.fr. L'administratrice de ce réseau, parvenue au restaurant par son téléphone portable, contacte Surcouf.

Pendant que Nau recopie un énorme fichier contenant des numéros de cartes bancaires factices, Surcouf installe un programme *Sniffer* sur pemmican.fr et consulte le compte de Nau dans cet ordinateur, car il a négligemment utilisé le même mot de passe pour tous ses comptes. Quelques minutes avant que Nau ait fini de recopier le fichier et se déconnecte, Surcouf retrouve le fichier de cartes bancaires volé sur le compte souscrit par Nau.

Les informations obtenues suffisent à la Direction de la surveillance du territoire, qui contacte le fournisseur et obtient l'identité de Nau. Munie de ces preuves, dont les comptes rendus détaillés fournis par le programme *Etherpeek*, le bureau du juge d'instruction délivre un mandat d'arrêt.

L'apportement de Nau est perquisitionné, et son ordinateur confisqué. Le disque dur de l'ordinateur révèle tout, même ce qui a été effacé. Un laboratoire identifie ses violations passées, notamment celle d'une grande institution bancaire parisienne.

Nau est mis en examen pour piratage informatique. Au procès, face à une juge intransigeante, Nau tente de négocier un compromis, malgré les dizaines de milliers de francs de dégâts occasionnés. Peine perdue, Jean Nau, dit l'Olonnais, purge aujourd'hui une peine de deux ans d'emprisonnement.

Carolyn MEINEL est écrivain scientifique spécialiste du piratage informatique.

Philippe BLANCHARD, *Pirates de l'informatique. Enquête sur les hackers français*, Milibert, 1995.

Æleen FRISCH, *Les bases de l'administration système*, deuxième édition, O'Reilly, 1996.

Jean GUINEL, *Guerres dans le cyberspace*, Découverte, 1997.

Craig HUNT, *TCP/IP, Administration de réseau*, deuxième édition, O'Reilly, 1998.

Cryptographie et réseau

PHILIP ZIMMERMANN

Les courriers électroniques et les diverses informations numériques envoyées sur le réseau Internet sont comme des cartes postales numériques : leur contenu n'est pas protégé. Des systèmes de cryptographie assurent le secret des transmissions électroniques.

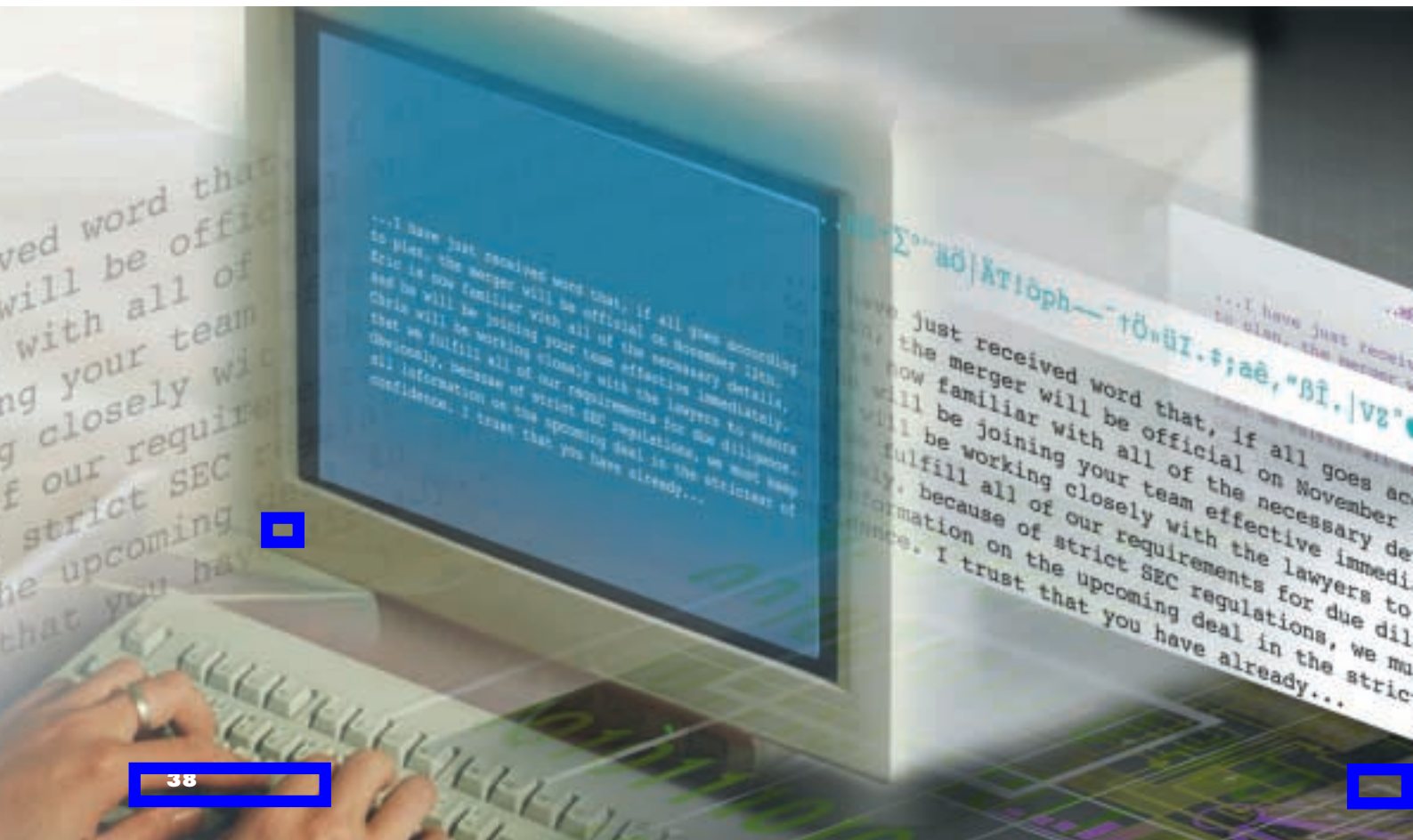
L'acheminement des lettres par la poste prend parfois des jours, voire des semaines, pour arriver à destination. À l'inverse, le courrier électronique arrive en un clin d'œil, mais il peut être lu par des indiscrets. Des systèmes de chiffrement peuvent toutefois assurer la confidentialité de telles transmissions : on mélange l'information de manière tellement complexe qu'elle devient inintelligible, excepté pour le destinataire légitime, qui connaît les règles du mélange.

Depuis les années 1980, les ordinateurs personnels sont si puissants qu'ils peuvent utiliser des systèmes

cryptographiques naguère réservés aux militaires. Ces systèmes sont aujourd'hui accessibles à tous.

Sortir de l'ombre

Avant le milieu des années 1970, l'Agence de sécurité américaine (NSA pour *National Security Agency*) avait le quasi-monopole de la cryptographie américaine ; les méthodes étaient confidentielles, connues seulement de quelques «hommes du chiffre». En 1976, un article intitulé *De nouvelles voies pour la cryptographie*, a ouvert la cryptographie



au monde de la recherche : en décrivant la «cryptographie à clé publique», les travaux de Whitfield Diffie et Martin Hellman, de l'Université de Stanford, ont suscité l'émergence d'une communauté universitaire et industrielle dynamique. Le développement du réseau Internet et le souci de confidentialité de ses utilisateurs ont intensifié les études de cryptographie civile. Aujourd'hui, les meilleurs algorithmes de chiffrement et les meilleurs systèmes cryptographiques sont mis en œuvre par les services de renseignement militaires américains achètent même des programmes de chiffrement pour leurs propres besoins.

Pourquoi l'introduction de la cryptographie à clé publique était-elle si importante? Dans les systèmes classiques, une même clé est utilisée pour le chiffrement et pour le déchiffrement. Avec ces «systèmes symétriques», la clé de chiffrement doit être transmise sur une ligne sécurisée, mais si l'on dispose d'une ligne sécurisée inviolable, pourquoi chiffrer les messages?

Grâce à la cryptographie à clé publique, la communication chiffrée est possible sans canal sécurisé pour l'échange des clés. Chaque message est chiffré avec une clé publique et une clé complémentaire. Chaque clé chiffre le message qui est déchiffré par l'autre clé ; le processus n'est pas réversible, car la clé utilisée pour chiffrer le message ne peut être utilisée pour le déchiffrement. La clé publique (la clé publique) peut être divulguée, tandis que l'autre (la clé secrète) n'est connue que de son propriétaire. Lorsque Bernard désire envoyer un message à Alice, il utilise la clé publique de cette dernière pour chiffrer le message. Alice utilisera ensuite sa clé secrète pour le déchiffrer.

La cryptographie à clé publique est fondée sur l'utilisation de problèmes mathématiques faciles à résoudre dans un sens, mais très difficiles dans le sens inverse. Les deux algorithmes à clé publique les plus célèbres sont l'algorithme

de Diffie et Hellman (ainsi que ses diverses variantes) et l'algorithme RSA, inventé par Ronald Rivest, Adi Shamir et Leonard Adleman, de l'Institut de technologie du Massachusetts.

L'algorithme de Diffie et Hellman est un algorithme de cryptographie à clé publique, c'est-à-dire que l'on calcule des valeurs du type $g^x \text{ modulo } p$. Un tel calcul est simple : on élève un nombre g à une puissance x , puis on divise le résultat par un grand nombre premier p et l'on conserve finalement le reste de la division.

table : même si l'on connaît les valeurs numériques de g , de p et de x , il est très difficile de retrouver x (voir *Les mathématiques de la cryptographie à clé publique*, par Martin Hellman, octobre 1979).

L'algorithme RSA, d'autre part, est fondé sur la factorisation des nombres : s'il est facile de multiplier deux grands nombres premiers, il est très difficile de décomposer le très grand nombre obtenu en ses deux facteurs premiers quand on ne les connaît pas.

Avec les algorithmes à clé publique, le destinataire peut connaître l'identité de l'expéditeur. Lorsque Bernard envoie

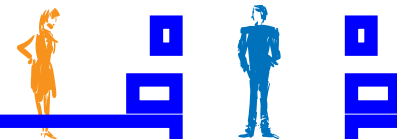
1. LE CHIFFREMENT D'UN MESSAGE que Bernard envoie à Alice par le réseau Internet s'effectue en plusieurs étapes. Tout d'abord, Bernard calcule un condensé de son texte (voir le diagramme de la page 39), puis il l'encadre en utilisant sa clé secrète (voir l'encadré de la page suivante). L'information résultante (en bleu ci-dessous) est la signature numérique du message de Bernard, une sorte d'empreinte digitale qui certifie que le message vient bien de Bernard. Cette signature et le message sont ensuite comprimés (en violet), puis chiffrés à l'aide d'une clé nommée clé de session. Bernard chiffre ensuite cette clé en utilisant la clé publique d'Alice et il ajoute le résultat (en orange) au message. Le fichier résultant est ensuite converti en caractères alphanumériques (en rouge), puis expédié sur le réseau. À la réception, les étapes sont inversées. Alice utilise sa clé secrète pour déchiffrer la clé de session qui servira à son tour à déchiffrer le reste du message.



un message à Alice, il le chiffre avec sa clé secrète, puis il chiffre le résultat en utilisant la clé publique d'Alice. À la réception, Alice effectue les étapes inverses : elle déchiffre le message avec sa clé secrète, puis elle déchiffre le résultat avec la clé publique de Bernard. Si elle parvient à lire le message, elle est certaine que c'est bien Bernard qui l'a écrit.

Ces opérations de chiffrement et de déchiffrement nécessitent des myriades d'opérations mathématiques, mais des logiciels exécutables par des ordinateurs personnels automatisent le processus ; l'utilisateur n'a qu'à cliquer sur les boutons «chiffrer» ou «déchiffrer» (ainsi mon programme PGP, l'acronyme de *Pretty Good Privacy*, soit «confidentialité raisonnable», est distribué gratuitement sur le réseau Internet ; son utilisation en France est maintenant autorisée).

Cryptographie à clé publique



ALICE x secret	BERNARD y secret
g^x	g^y
$(g^y)^x$	$(g^x)^y$
Le secret partagé est g^{xy}	

Pendant des siècles, la cryptographie a été handicapée par le problème de l'échange des clés. Supposons que Bernard ait envoyé un message chiffré à Alice. Cette dernière ne pourra lire le message que si elle reçoit également la clé de codage. Les systèmes cryptographiques à clé publique évitent cet envoi, grâce à l'utilisation de mathématiques ingénieuses.

Avec l'algorithme de Diffie et Hellman, Alice utilise son nombre secret x pour calculer g^x (où g est un nombre public) et elle envoie cette valeur à Bernard. De son côté, Bernard utilise son nombre secret y pour calculer g^y et envoie le résultat à Alice. À la réception, Alice peut alors calculer $(g^y)^x$, tandis que Bernard calcule le même nombre $(g^x)^y$. Cette quantité donne leur clé secrète partagée.

Un intrus qui aurait intercepté la valeur g^x d'Alice, ainsi que la valeur g^y de Bernard peut en déduire les valeurs secrètes de x et de y . Aussi, pour déjouer toute indiscrétion, Alice et Bernard utilisent la formation modulo, qui donne le reste d'une division (par exemple, 14 modulo 4 est égal à 2 : le reste de la division de 14 par 4 est égal à 2). Cette astuce assure le secret, car, au lieu d'envoyer g^x à Bernard, Alice lui transmet le nombre g^x modulo p , à partir duquel un pirate aura bien du mal à retrouver x , même s'il connaît g et p .

En compliquant l'algorithme de Diffie et Hellman, on a obtenu des systèmes qui engendrent deux clés complémentaires, l'une secrète (x pour Alice) et l'autre publique (à savoir g , p et g^x modulo p). La clé secrète déchiffre le message chiffré par la clé publique, mais la clé utilisée pour chiffrer un message ne peut être utilisée pour le déchiffrer. Ainsi, Bernard peut utiliser la clé publique d'Alice (qu'elle a donnée à tout le monde) pour chiffrer un message qui lui est destiné, mais seule Alice peut déchiffrer ce message à l'aide de sa clé secrète.

Malgré ces progrès, la cryptographie à clé publique a deux graves limitations. D'une part, la technique est relativement lente, de sorte qu'en pratique on ne peut chiffrer les messages trop longs. D'autre part, des structures mathématiques du message en clair subsistent dans le message chiffré. Détectables dans le texte chiffré, ces fragments sont utilisables par des spécialistes, qui peuvent reconstituer la totalité des messages.

Chevaux de bataille symétriques

Pour ces raisons, on préfère les techniques symétriques, plus rapides et plus sûres, et la cryptographie à clé publique ne sert que lors de l'étape d'échange des clés symétriques. Par exemple, Bernard chiffre son message avec une clé symétrique rapide et sûre. Comme il doit envoyer à Alice la clé qu'il a utilisée, il la chiffre avec la clé publique d'Alice et attache le résultat à son message chiffré. Alice pourra déchiffrer la clé symétrique en utilisant sa clé secrète. Muni de la clé symétrique, elle déchiffre alors le reste du message de Bernard.

Pour authentifier ses messages, Bernard ne les signe pas non plus à l'aide des techniques à clé publique ; il extrait du message un condensé, appelé «empreinte digitale», à l'aide d'une transformation mathématique, nommée fonction de hachage. Cette transformation associe à un message de longueur quelconque un message de longueur fixe, telle que 160 bits (un bit est un chiffre binaire, égal à 0 ou à 1). Les programmes cryptographiques sont conçus de manière que deux messages différents n'aient pas le même condensé. Autrement dit, l'empreinte digitale est unique, deux messages différents ayant à peu près certainement une empreinte différente.

Après avoir calculé le condensé de son message, Bernard le chiffre avec sa clé secrète. Il envoie cette «signature» en même temps que le reste de son message chiffré. Lorsqu'elle reçoit ce condensé chiffré, Alice le déchiffre grâce à la clé publique de Bernard. Elle compare alors le résultat obtenu avec le résultat qu'elle calcule elle-même après déchiffrement du message. Si les deux résultats sont identiques, elle conclut que le message n'a pas été modifié et que Bernard en est bien l'expéditeur.

Pour coder les messages, on les découpe souvent en blocs de taille fixe (généralement 64 ou 128 bits), puis on chiffre individuellement les blocs successifs. Ce système de chiffrement par blocs crypte plusieurs fois chaque bloc (le nombre d'itérations dépend des algorithmes utilisés). Chaque itération fait intervenir des permutations circulaires (la permutation d'un groupe de trois blocs «xtv» devient «tvx») et des substitutions («tvx» engendre «cb2»). Une permutation déplace les bits d'un groupe de bits, les données au cours de chaque itération.

Quand on fournit des morceaux de texte identiques à un système de chiffrement par blocs, on obtient des blocs identiques. Aussi, afin d'éviter le maintien de structures qui faciliteraient la découverte du message, les algorithmes par blocs utilisent un chaînage : les blocs qui viennent d'être chiffrés servent à déchiffrer les blocs suivants. Le chiffrement d'un bloc de texte dépend alors de tous les blocs qui le précèdent.

La longueur des clés de chiffrement par blocs est généralement égale à 56, 128 ou 256 bits. Les méthodes les plus connues sont DES (*Data Encryption Standard*, soit

«standard de chiffrement de données»), triple-DES, CAST, IDEA et *Serpent*. Les algorithmes par blocs sont au centre de la plupart des recherches actuelles en cryptographie.

La clé est la clé

En cryptographie, l'étape la plus sensible est la création des clés. Pour qu'un système soit le plus sûr possible, les clés doivent être des nombres réellement aléatoires, imprévisibles par un éventuel pirate. Les séquences pseudo-aléatoires déterministes que les ordinateurs engendrent pour les jeux ou les simulations sont inutilisables, car ils sont insuffisamment aléatoires. La seule manière d'engendrer de vrais nombres aléatoires est d'utiliser un «bruit» physique, telle la désintégration radioactive.

À l'aide d'un ordinateur, on fabrique difficilement des nombres aléatoires aussi bons que ceux issus de la physique. On obtient toutefois des résultats raisonnables quand on utilise l'intervalle de temps, en microsecondes, qui sépare la frappe de deux touches d'un clavier : cette valeur est impossible à prédire. Les données obtenues ainsi ne sont pas assez aléatoires pour fabriquer directement des clés, mais peuvent être transformées pour accroître le désordre.

La seule méthode cryptographique dont on ait prouvé la parfaite sécurité est le chiffrement de Vernam, où la longueur de la clé est égale à la longueur du message. Dans cette méthode, on utilise une séquence aléatoire pour chiffrer le message. Par exemple, si la clé est 10110101 et le message 11010101, la clé code le 34^e bit du message. La clé doit être parfaitement aléatoire, elle ne peut pas être une séquence pseudo-aléatoire issue d'un algorithme déterministe, sinon le code pourrait facilement être cassé. Le chiffrement de Vernam est rarement utilisé, en raison de difficultés pratiques : la clé, qui est aussi longue que le message, doit être envoyée au destinataire par un canal de transmission sûr. De surcroît, on ne peut utiliser chaque clé qu'une seule fois, sinon un pirate pourrait la décrypter.

Si la taille des clés détermine l'efficacité des systèmes cryptographiques, la conception des systèmes est également très importante. Considérons un simple code de substitution où tous les A seraient transformés en W, tous les B en K, tous les C en Q, et ainsi de suite. Le nombre de façons différentes d'attribuer les lettres est $26!$ (lire «factorielle 26», est égal à $26 \times 25 \times 24 \dots 3 \times 2 \times 1$), soit environ 4×10^{26} (un nombre de 26 chiffres)! On ne peut tester toutes les combinaisons une à une, mais, lorsque j'étais enfant, je m'amusais à casser ce type de code avec un papier et un crayon : je regardais simplement la lettre la plus fréquente et je supposais qu'il s'agissait d'un E ; puis je cherchais la deuxième lettre la plus fréquente et je supposais que c'était un S. En fait, ce type de code est très simple.

En fait, la sécurité d'un système cryptographique n'est pas proportionnelle à la taille de la clé. Par exemple, dans un système par blocs, par exemple, la relation est plutôt exponentielle : un **code de plus d'une douzaine de chiffres** peut éventuellement doubler le nombre d'essais. L'effort nécessaire est élevé au carré quand la taille de la clé est doublée. Pour casser un système qui utilise une clé de longueur 128 bits, il faut en moyenne 2^{127} (soit $1,7 \times 10^{38}$) opérations.

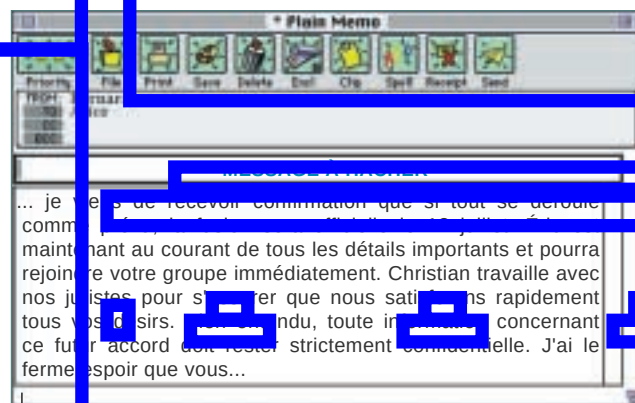
Pour les algorithmes à clé publique, la difficulté augmente plus lentement. L'espace des clés augmente moins vite qu'une loi exponentielle, mais plus vite qu'une loi de

puissance. Le doublement de la longueur de la clé n'élève pas autant l'effort à fournir pour casser le code, mais le travail reste considérable. Par exemple, dans le système RSA, les algorithmes modernes de factorisation peuvent faire beaucoup mieux que d'essayer toutes les combinaisons de nombres premiers possibles pour factoriser un nombre de grande taille. Le code de Diffie et Hellman est, lui aussi, «sous-exponentiel». Par exemple, une clé de 3 000 bits pour RSA ou Diffie-Hellman est aussi difficile à décrypter qu'une clé de 128 bits d'un système de chiffrement par blocs.

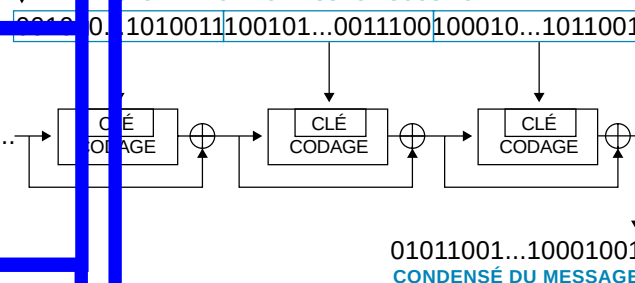
Le chiffrement par blocs n'est toutefois pas invulnérable. En 1996, la *Société Electronic Frontier Foundation* a construit, pour moi, un **crackeur** qui a cassé un message chiffré par DES en explorant toutes les clés à 56 bits en moins d'une semaine.

La recherche de la clé est souvent la partie la plus difficile du code. Des méthodes mathématiques élaborées et des outils statistiques raccourcissent le travail. Certaines méthodes recherchent, par exemple, un motif particulier dans le message chiffré. Ces méthodes statistiques sont classées en trois catégories selon ce qui est connu du texte clair et du texte chiffré.

Quand le pirate connaît seulement le message chiffré, il n'a rien pour le guider dans sa recherche de la clé, si bien que même un système simple de chiffrement résiste aux



TRANSFORMATION DU MESSAGE SOUS FORME BINAIRE



2. UNE FONCTION DE HASHAGE crée un condensé de message, semblable à une empreinte digitale utilisée pour détecter les falsifications. Le texte d'un message est d'abord converti en chiffres binaires (la lettre A peut être représentée par 00000, la lettre B par 00001, le C par 00010, etc.) ; puis la suite de caractères qui en résulte est découpée en blocs de taille fixe. Chacun des blocs sert alors de clé dans un système de codage. La sortie finale est le condensé du message original. Quelle que soit la longueur du message initial, le condensé a toujours la même taille. C'est une opération à sens unique, car il est quasi impossible de retrouver le message original à partir de son condensé. De surcroît, avec cet algorithme, deux messages donnent presque toujours des condensés différents et il est impossible de trouver un autre message ayant le même condensé : ce condensé est une «empreinte digitale» du message.

assauts. En revanche, quand le pirate connaît au moins une partie du message, ses chances de succès augmentent. Par exemple, s'il sait qu'il commence par «Cher Monsieur Dupond», il peut d'abord chercher une clé qui décrypte la partie «Cher Monsieur Dupond» du texte clair, puis poursuivre le décryptage à l'aide des informations trouvées.

Même quand le pirate ne connaît que le langage utilisé dans le texte clair, russe, français ou COBOL, il peut exploiter cette information. Si le message est en français, par exemple, alors le mot le plus fréquemment utilisé est sans doute «le» ou «à». Pour déjouer de telles attaques, certains systèmes cryptographiques compriment le message en clair,

Les certificats numériques sont importants en cryptographie à clé publique, parce qu'ils garantissent qu'un intermédiaire n'espionne pas les échanges. Pour envoyer ou recevoir des messages en utilisant des clés publiques, un utilisateur doit posséder deux clés cryptographiques, l'une secrète, l'autre publique. Ces clés sont de longues suites de 0 et de 1 (entre 500 et 1 000 chiffres binaires). L'utilisateur garde sa clé secrète dans un endroit sûr, chiffrée sur un disque dur par exemple, mais il distribue sa clé publique à ceux avec qui il veut communiquer.

Supposons qu'Alice veuille envoyer à Bernard un message authentifié, c'est-à-dire un message dont Bernard saura de façon certaine qu'il vient d'elle. En utilisant sa clé secrète, Alice

crée une signature numérique qu'elle joindra au message. Puis, en utilisant la clé publique d'Alice, Bernard vérifie cette signature. Cependant, comment Bernard saura-t-il que la clé publique appartient effectivement à Alice ?

Un imposteur pourrait créer sa propre paire de clés et envoyer sa clé publique à Bernard en prétendant qu'elle appartient à Alice. On évite cette fraude en utilisant une autorité de certification, qui fournira un certificat numérique sur la clé publique reconnue par tous. Plusieurs entreprises, telles *VeriSign* ou *GTE CyberTrust*, délivrent des certificats numériques. Ainsi, le certificat numérique est l'analogue informatique de la carte d'identité.

Warwick FORD, *VeriSign*

1. À l'aide des logiciels de cryptographie, Alice crée une clé secrète (a) ainsi qu'une clé publique (b). Elle envoie la clé publique à une autorité de certification, à qui elle demande un certificat numérique. Pour authentifier Alice, cet organisme vérifie les informations fournies par Alice. Si tout est en ordre, l'organisme de certification envoie un certificat numérique (c) qui authentifie la clé publique d'Alice. Sur ce certificat se trouve la signature numérique du tiers de confiance qui peut être vérifiée par toute personne connaissant la clé publique de cet organisme.

2. La clé publique (d) de l'autorité de certification est fournie à ceux qui en ont besoin, dont Bernard. Elle peut être incluse dans les programmes de navigation sur le réseau Internet et dans d'autres logiciels utilisés pour les communications informatiques sécurisées.

3. Alice signe numériquement le message qu'elle envoie à Bernard. Tout d'abord, elle crée un condensé du message en lui appliquant une fonction de hachage. Le condensé ainsi créé est ensuite chiffré à l'aide de la clé secrète d'Alice ce qui donne la signature numérique du message (e). Cette signature est envoyée à Bernard en même temps que le message (f). Alice envoie aussi son certificat numérique, qui contient sa clé publique.

4. Bernard utilise la clé publique correspondant à l'autorité de certification pour vérifier la signature numérique officielle apposée sur le certificat. Il est alors certain que le certificat est authentique et que la clé publique qui l'accompagne appartient à Alice. Il utilise alors cette clé pour déchiffrer la signature numérique d'Alice et obtient donc le condensé du message. Il applique la fonction inverse au message envoyé par Alice et obtient ainsi un condensé du message. Si ce condensé est identique à celui qui est obtenu par le déchiffrement de la signature numérique d'Alice, Bernard est certain que le message provient bien d'Alice et qu'il n'a pas été altéré par une tierce personne.

préalablement au chiffrement, ce qui en enlève les motifs prédictibles.

Souvent le pirate en connaît bien plus. S'il a volé une carte à puce qui contient un système cryptographique, il peut envoyer à la carte des milliards de messages judicieusement choisis et étudier les messages chiffrés correspondants. De telles attaques percent facilement les systèmes de chiffrement peu efficaces. Dans le cas des systèmes à clé publique, le pirate peut intercepter les messages échangés avec la clé publique (connue) et analyser le texte chiffré qui en résulte. Des méthodes d'analyse des systèmes de chiffrement performantes apparaissent depuis peu : ce sont les méthodes différentielles et linéaires. On les a utilisées pour analyser un grand nombre de systèmes de chiffrement par blocs et pour montrer qu'il est possible de décrypter les messages chiffrés à l'aide de l'algorithme DES des centaines ou des milliers de fois plus rapidement que par une recherche exhaustive.

Dans la cryptanalyse différentielle, introduite par A. Shamir et Eli Biham, de l'Institut Weissman, en Israël, on code des paires de messages chiffrés, puis on les soustrait. On choisit judicieusement les paires de messages chiffrés, afin de trouver des différences dans les paires chiffrées. La découverte de ces différences renseigne alors sur la clé. Dans la cryptanalyse linéaire, on se sert d'un point par Mitsuru Matsui, de la Société *Mitsubishi*, on recherche les corrélations, même faibles, qui existent entre les textes clairs, les textes chiffrés et les clés. La méthode accumule les statistiques obtenues sur un grand nombre de couples texte clair-texte chiffré, à la recherche de tendances qui donneraient des indices sur la clé.

Attention aux intermédiaires

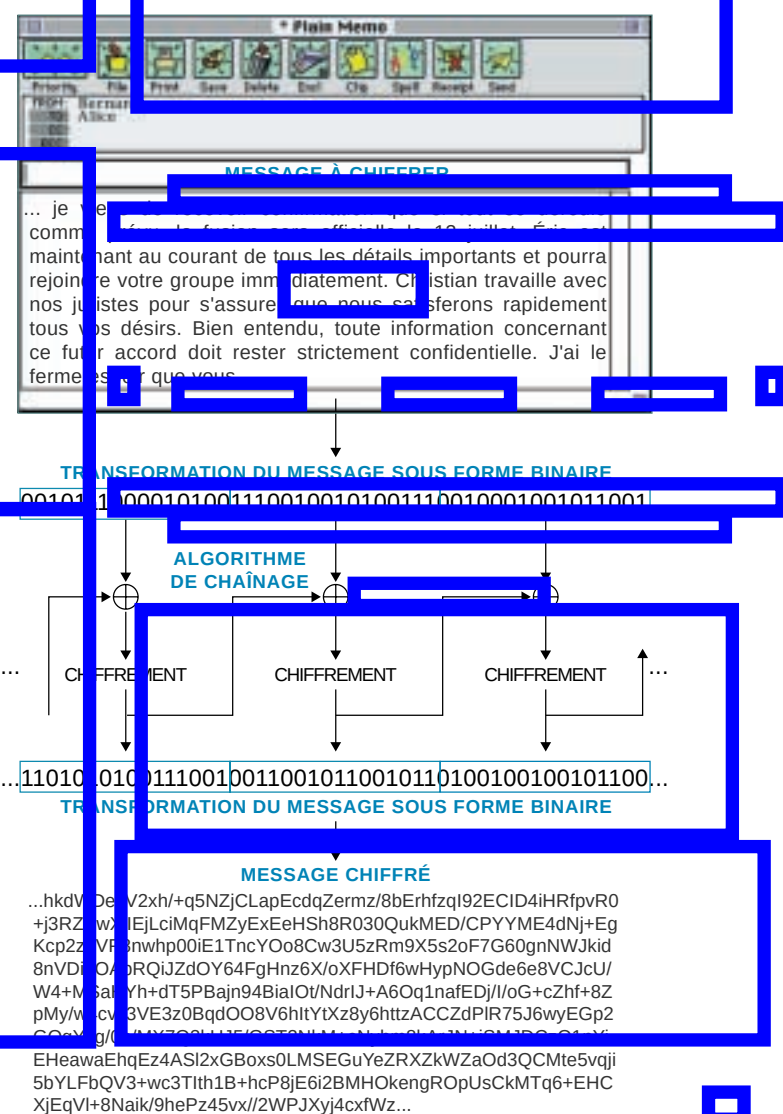
Bien qu'efficaces, les méthodes de cryptanalyse (l'étude de la façon de percer les messages secrets) nécessitent de nombreux essais. Si le système de chiffrement est robuste, les pirates préfèrent attaquer son implémentation, car elle laisse parfois « fuir » de l'information. Les systèmes cryptographiques à clé publique sont très vulnérables à une attaque par un tiers qui s'interposerait dans la communication. Bernard, qui envoie un message à Alice, peut ignorer que Caroline s'interpose. Si Caroline parvient à faire croire à Bernard que sa propre clé publique est celle d'Alice, elle pourra déchiffrer les messages émis par Bernard.

Bernard ne peut éviter cette intrusion qu'en s'assurant que la clé utilisée est bien celle d'Alice. La complexité des bons systèmes de cryptographie à clé publique vise presque uniquement à donner cette garantie. Certains systèmes cryptographiques font appel à un tiers de confiance, qui certifie les clés. Toutefois, les clés doivent-elles être certifiées de manière descendante, par des autorités gouvernementales, ou de manière centralisée, au choix des utilisateurs de systèmes cryptographiques ?

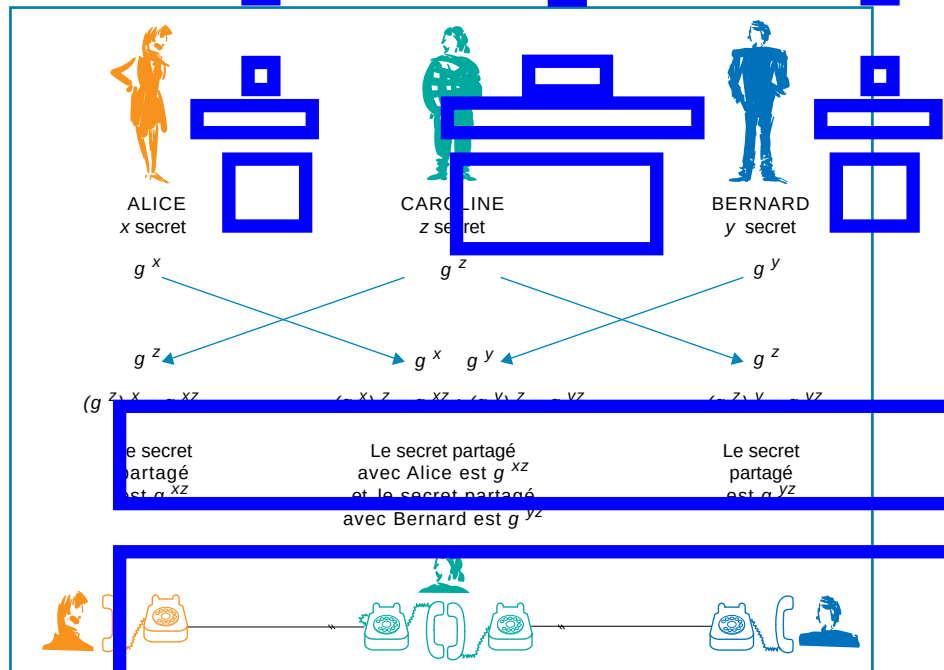
Les algorithmes de cryptographie se sont améliorés en même temps que la cryptanalyse. Le système DES, arrivé en fin de vie, surtout en raison de sa petite clé de 56 bits et de ses blocs de 64 bits, sera remplacé par un nouveau système cryptographique, l'AES (*Advanced Encryption Standard*, soit « standard de chiffrement avancé »). Ce système, qui a mis la communauté de la cryptographie en effervescence, devrait utiliser des clés de 128, 192 ou 256 bits pour chiffrer des données en blocs de 128 bits.

Les systèmes AES devront satisfaire plusieurs contraintes. Ils devront utiliser plusieurs longueurs de clés et de blocs ; ils devront être rapides, créant les clés, chiffrant et déchiffrant les messages à l'aide de processeurs 32 bits, tels ceux qui équipent les ordinateurs personnels, ou de microprocesseurs 8 bits, tels ceux des cartes à puce ; enfin, ils devront fonctionner correctement lors des échanges sur le réseau, par exemple, par satellite.

Plusieurs propositions d'AES sont intéressantes. Elles bénéficient des études du codage par blocs et des recherches de défense contre les méthodes de cryptanalyses différentielles et linéaires. Plusieurs des 15 systèmes proposés seraient efficaces. Le système MARS, qui dérive du système DES de la Société *IBM*, utilise deux structures très différentes pour chaque itération de chiffrement. Cette approche mixte permet, selon la Société *IBM*, une sécurité



3. DES ALGORITHMES DE CHAÎNAGE améliorent la sécurité des techniques de chiffrements par blocs. On transforme d'abord un message en une chaîne de 0 et de 1 ; puis on découpe cette longue séquence en blocs de même taille. Avant de chiffrer chacun de ces blocs, on le combine mathématiquement avec le bloc chiffré précédent. Ainsi, le chiffrement du 23^e bloc dépend du 22^e bloc chiffré, qui dépend lui-même du chiffrement du 21^e, et ainsi de suite. Le chiffrement d'un bloc dépend alors de tous les blocs précédents.



4. LES SYSTÈMES CRYPTOGRAPHIQUES À CLÉ PUBLIQUE sont vulnérables. Interceptant les transmissions entre Alice et Bernard, l'espionne Caroline dupe Bernard en utilisant son propre g^z à la place du g^x d'Alice et trompe Alice en utilisant g^z à la place du g^y de Bernard (voir l'encadré de la page 40). Elle déchiffre et rechiffre à leur insu les messages qu'ils échangent.

que n'autorisent pas les systèmes de chiffrement classiques. Le procédé CAST-256 est un chiffre à clé publique, basé sur le système de chiffrement de Rivest, Shamir et Adleman (RSA) et à des blocs de 128 bits. Le système *Twofish* est mathématiquement plus rigoureux que *Blowfish*, son prédécesseur. La conception de *Serpent* est fondée sur un principe de «double diffusion», qui permet d'engendrer très rapidement des clés autorisant ainsi son utilisation en tant que fonction de hachage. Au département de mathématiques et d'informatique de l'École normale supérieure, l'équipe de Serge Vaudenay a mis au point le système DFC (*Decorrelated Fast Cipher*, soit «codage décorrélaté rapide»), très rapide, et dont on peut prouver la sûreté face à certains types d'attaques.

Déchiffrer le futur

Quelle que soit la proposition sélectionnée, AES avantagera les utilisateurs. Aujourd'hui, les meilleurs systèmes de cryptographie sont supérieurs aux meilleures méthodes de cryptanalyse connues. Bien sûr, la cryptanalyse viendra à bout de tout système de chiffrement, mais l'écart entre les méthodes de chiffrement et les méthodes de «cassage» se creusera progressivement.

Je partage cette opinion : la cryptographie civile a grandi dans les universités et dans les entreprises privées, et elle a rattrapé la cryptographie militaire. D'ailleurs, les militaires américains ont rendu public leur système de chiffrement *Skipjack*, qu'ils avaient mis au point en secret. Selon une étude d'Eli Bihani, cet algorithme serait moins sûr que les meilleurs algorithmes universitaires. Comme le réseau Internet, la cryptographie est sortie du giron militaire. Souhaitons-lui une croissance aussi remarquable!

Philip ZIMMERMANN est l'auteur du programme de chiffrement PGP (*Pretty Good Privacy*). Il travaille pour la Société *Network Associates*.

Bruce SCHNEIER, *Cryptographie appliquée*, Vuibert, 1996.

Doug STINTON, *Cryptographie : théorie et pratique*, Vuibert, 1996.

G. DUBERTRET, *Initiation à la cryptographie*, Vuibert, 1998.

Paielements sur l'Internet

OCTAVIAN URECHE • RÉJEAN PLAMONDON

L'essor du commerce électronique nécessite de nouveaux moyens de paiement numériques, adaptés au monde virtuel de l'Internet

La croissance du commerce sur le réseau Internet est phénoménale : en 1997, le total des achats a atteint 80 milliards de francs dans le monde et, en 2002, ce chiffre atteindrait près de 3 000 milliards de francs. Les communications étant aujourd'hui faciles et rapides, les informaticiens cherchent à faciliter les transactions monétaires.

Ce type de communications nécessite un niveau minimal de confiance, tant de la part des consommateurs que de la part des fournisseurs. Les cartes de crédit, chèques ou portefeuilles virtuels ne puissent tomber dans les mains d'un tiers malintentionné, et que les biens et services achetés « en ligne » soient livrés ; les fournisseurs de biens et services veulent la garantie qu'ils recevront les fonds qui correspondent aux marchandises vendues. Aujourd'hui, la sécurisation du paiement est essentiellement assurée grâce au chiffrement : les données transactionnelles sont chiffrées, et leur validité peut être vérifiée à l'aide des signatures numériques.

Outre les protocoles de transaction sécurisés requièrent des protocoles de transaction qui dépendent de la représentation monétaire : cartes de crédit, chèques ou argent virtuel. Si la plupart des systèmes de paiement numérique sur l'Internet inspirent des systèmes classiques de paiement du « monde réel », plusieurs systèmes introduisent de nouveaux moyens de transaction dans le monde virtuel.

Après avoir examiné et évalué divers systèmes électroniques de paiement sur l'Internet, nous décrirons un nouvel instrument transactionnel, nommé *TRANZIX*, qui généralise les notions utilisées habituellement dans ces systèmes, et qui offre un compromis raisonnable entre le besoin de confidentialité des consommateurs et le besoin de transparence que réclament les États pour lutter contre le crime organisé et, notamment, le blanchiment d'argent.

Concrètement, les protocoles de transaction de compromis : les informations de trace, qui permettent de retracer le parcours d'une transaction en général et d'un bien en particulier, et les moyens cryptographiques, qui offrent une réelle confidentialité aux usagers, en dissimulant ces traces, de façon à les rendre invisibles pour tout accès non autorisé.

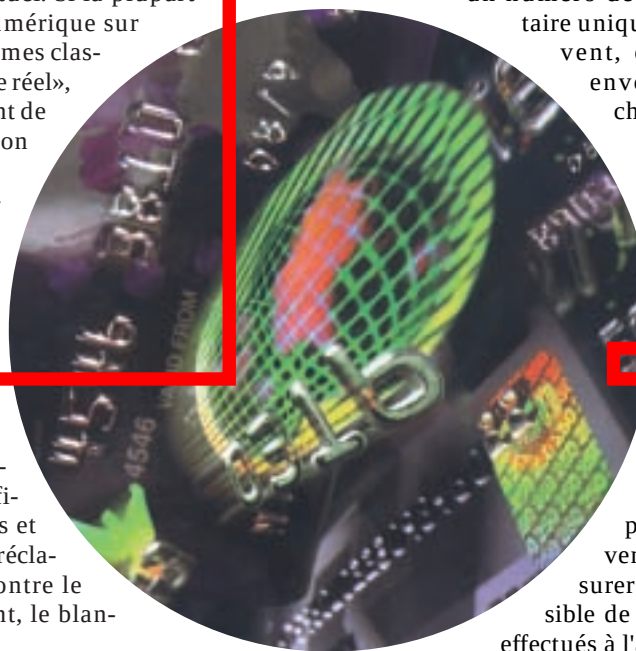
Représentation monétaire

Selon le modèle transactionnel, on trouve plusieurs représentations monétaires. Ainsi, le paiement peut se faire à l'aide de cartes de crédit virtuelles : le numéro d'une carte de crédit « réelle » est chiffré, puis envoyé avec un certificat numérique (voir l'encadré de la page 42). Les protocoles fondés sur le standard SET (Secure Electronic Transactions), soit « transactions électroniques sécurisées » soutenu par des sociétés telles que Visa et MasterCard.

L'équivalent virtuel du chèque est le chèque électronique. Les informations à transmettre comprennent alors un numéro de compte bancaire, un destinataire unique et une date d'expiration. Souvent, ces chèques sont imprimés, envoyés ou encaissés comme des chèques réels.

Une nouvelle forme de représentation monétaire reproduit fidèlement l'argent comptant : c'est l'argent virtuel. L'argent virtuel est constitué de fichiers binaires qui contiennent plusieurs renseignements, parmi lesquels :

plusieurs signatures numériques. Comme dans le monde réel, ce type de représentation monétaire a la particularité d'appartenir « au porteur » et, très souvent, on y inclut des moyens d'assurer l'anonymat ; il est donc impossible de retracer les transferts des fonds effectués à l'aide de l'argent virtuel.



Ces représentations monétaires sont échangées à l'aide de systèmes transactionnels qui doivent empêcher l'accès non autorisé aux données – et aux fonds – privées des utilisateurs. Le chiffrement et le contrôle d'accès, tel le mot de passe, protègent relativement bien contre ce type d'intrusion. En revanche, le problème des «dépenses multiples» est plus ardu. Comment empêcher un utilisateur de copier plusieurs fois et dépenser auprès de différents vendeurs de façon illicite? Aujourd'hui, on effectue le contrôle en utilisant le numéro de série du billet et des coordonnées des utilisateurs des billets, qui sont toujours inclus dans les protocoles de paiement au moyen d'argent virtuel. L'émetteur du billet dissuade ainsi les fraudeurs putatifs, qui peuvent être retrouvés. Toutefois, dans les systèmes classiques, aucune donnée n'est fournie sur l'historique du billet ou sur sa date d'expiration.

Récemment, la Société Netscape Communications a introduit le concept de micropaiement. Ce système, nommé *MilliCent*, utilise des «coupons virtuels» qui abaissent le montant minimal d'une transaction. En utilisant ces coupons de réduction dans le «monde réel», ces coupons ne sont utilisables qu'auprès de leur magasin émetteur. Des paiements de quelques centimes sont ainsi possibles. Ce type de transactions ouvre des nouvelles possibilités : les entreprises pourraient faire payer la recherche d'une information, comme une cotation boursière par exemple.

La transaction

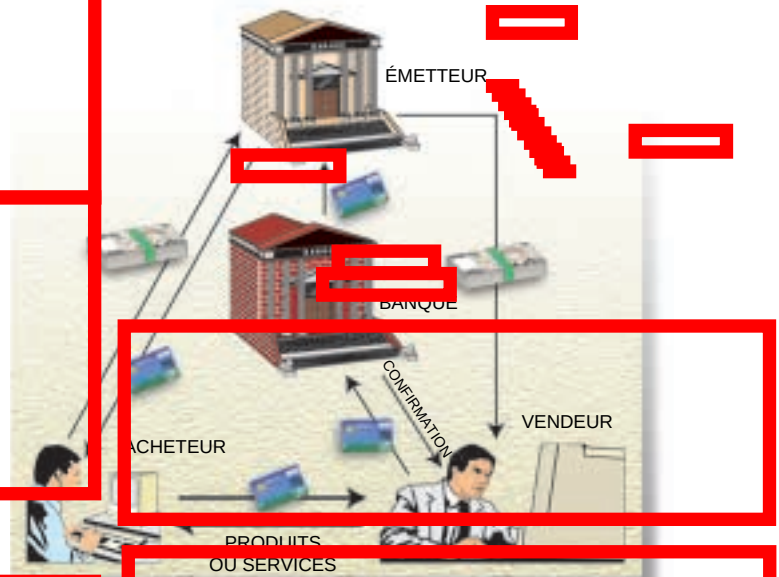
Comment effectuer une transaction sur Internet? Les acteurs y participent : un acheteur, qui désire échanger son argent contre des biens ou des services offerts en ligne ; le vendeur, qui offre ces biens ou ces services ; un intermédiaire, ou courtier virtuel, qui traite les transactions ; une banque, qui gère les comptes des clients et acquitte les transactions ; enfin un émetteur – généralement une banque –, qui émet la représentation monétaire utilisée dans le système de paiement. Par exemple, la représentation monétaire est, ainsi, les valeurs qu'elle représente.

Par exemple, dans le monde réel, la représentation monétaire émise par la *Deutsche Bundesbank* est le Deutsche Mark qui a, selon les analystes financiers, une qualité supérieure à celle du rouble russe ou du peso chilien ; cette qualité supérieure résulte non seulement d'une très bonne qualité d'impression et de l'utilisation d'un bon papier, mais surtout du fait que le papier est émis par une institution qui inspire confiance.

De façon générale, un client envoie la représentation monétaire au vendeur, qui la vérifie en l'envoyant à l'intermédiaire ou directement à la banque. Selon le résultat de cette vérification, le vendeur reçoit – le cas échéant – une confirmation et envoie alors la marchandise au client. L'acheteur achète cette représentation monétaire auprès de l'émetteur (voir la figure 1).

L'évaluation du paiement

Au vu du nombre croissant de systèmes numériques de paiement, leur évaluation est primordiale pour tous ceux qui veulent déployer et utiliser de tels systèmes transactionnels. Pour ce faire, nous avons proposé une taxonomie des systèmes de paiement numérique sur l'Internet.



1. LES SYSTÈMES DE PAIEMENT CLASSIQUES nécessitent en général quatre acteurs. L'acheteur achète des biens et des services à l'aide d'une représentation monétaire (carte de crédit virtuelle, chèque électronique, argent virtuel, etc.). Le vendeur est crédité de la somme correspondante par l'émetteur de la représentation monétaire, après vérification par une banque ou par un intermédiaire. La sécurité de la transaction dépend de la représentation monétaire et du type de vérification.

Dans notre classification, les systèmes se divisent en deux catégories : les systèmes de paiement par adhésion ou par adhésion de l'acheteur. Chacune des deux catégories contient plusieurs classes selon le modèle transactionnel et le niveau de protection – par exemple, le modèle sans protection, le modèle «débit-crédit», le modèle comptant, etc. Chaque classe contient un ou plusieurs groupes de systèmes de paiement reflétant la technique de transfert de fonds employée – par exemple, les systèmes fondés sur les mots de passe, les chèques électroniques, la facturation et les cartes de crédit, l'argent virtuel, etc.

Comment évaluer les systèmes transactionnels? À l'aide de leurs caractéristiques. On distingue les caractéristiques internes, les caractéristiques externes et les caractéristiques de sécurité. Les caractéristiques internes sont la sécurité, la représentation monétaire, la pérennité de cette représentation, sa «granularité» (la plus petite quantité que l'on peut échanger, surtout importante pour les micropaiements), la configuration du système et le niveau d'anonymat. Dans les caractéristiques externes, on inclut des éléments tels que le délai d'encaissement, le mode d'échange des fonds ou la convertibilité de la représentation monétaire.

Aujourd'hui, le protocole de sécurisation des communications transactionnelles le plus répandu est le protocole SSL (Secure Sockets Layer, «couche de sécurité»). Introduit en 1994 par la Société Netscape Communications, ce protocole est intégré dans les navigateurs les plus courants, tels *Netscape Navigator* et *Microsoft Internet Explorer*. Ce système est relativement sûr : en Europe, le protocole SSL chiffre les données avec des clés de 40 bits. Autrement dit, pour percer le code de chiffrement, il faudrait trouver les facteurs premiers d'un nombre de 40 bits (ou 10 chiffres), ce qui prendrait des jours à un ordinateur de bureau.

Pour les utilisateurs équipés de ces navigateurs, le chiffrement est transparent : lorsqu'un utilisateur entre son numéro de carte bancaire sur un site sécurisé (reconnais-
sable à l'adresse *https://*), le numéro est chiffré automatiquement par l'ordinateur de l'utilisateur, puis il transite sur le réseau et il est décrypté par la machine du serveur. Cette ergonomie explique la percée de ce système, mais l'utilisation des cartes de crédit réelles restreint son usage à ceux qui en détiennent. De surcroît, avec les cartes de crédit, seuls les montants supérieurs à 50 francs sont économiquement viables, de sorte que ce système n'est pas intéressant pour l'achat d'articles de journaux en ligne, par exemple.

Autre restriction de ce système transactionnel, il n'offre pas la non-répudiation (un usager pourrait prétendre ne pas avoir effectué une transaction). La communication est protégée : l'accès aux informations transactionnelles – notamment aux numéros des cartes de crédit utilisées – étant accessible aux vendeurs et aux intermédiaires, le niveau de sécurité de ce système est considéré comme faible. Dans une boutique à l'aide d'une carte de crédit possède un niveau de sécurité analogue : la facture où figure votre numéro de carte et sa date d'expiration est également accessible au vendeur.

Le système de paiement proposé par la Société *CyberCash* corrige certaines faiblesses du protocole SSL par l'ajout d'un «porte-monnaie électronique». De cette manière, *CyberCash* assure l'authentification des intervenants et un niveau raisonnable de non-répudiation des

transactions, aspect totalement absent de SSL, qui n'est qu'un protocole cryptographique utilisé pour sécuriser les communications. La solution française *Klebox* possède les caractéristiques analogues.

Les cartes à puce

Les cartes à puce sont bien connues en Europe depuis près de 20 ans. Utilisées principalement comme cartes bancaires et téléphoniques, elles trouvent une nouvelle utilisation comme moyen ergonomique de paiement sur l'Internet. La Société britannique *Mondex* va permettre l'utilisation sur l'Internet de sa carte de paiement : à l'aide de lecteurs spécifiques branchés sur un port de communication, elle permet des transactions sécuritaires. Le niveau de sécurité de ce système est élevé. La disponibilité, l'intégrité, la confidentialité et l'authentification sont assurées par des techniques cryptographiques. Seul le critère de non-répudiation n'est pas respecté, car un usager pourrait prétendre ne pas être celui qui a effectué la commande. Si les projets pilotes sont des succès, cette méthode sera généralisée à des transactions à l'aide de cartes à puce classiques.

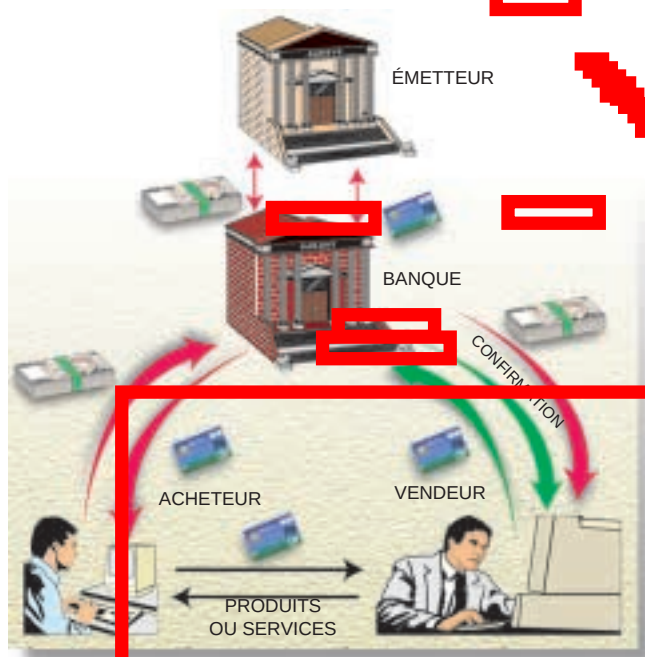
Un niveau de sécurité encore supérieur a été mis au point par la Société hollandaise *DigiCash*. Le système, nommé *eCash*, utilise le concept d'argent électronique pour le paiement sur l'Internet. Il s'agit de pièces de monnaie virtuelles que l'on achète avec de l'argent réel (moyennant un transfert bancaire par exemple) et que l'on échange à chaque achat contre des produits et des services. Une méthode qui assure la confidentialité de l'information, et un système de signatures numériques assure l'intégrité de l'information, l'authentification des intervenants et la non-répudiation des transactions. De surcroît, le système permet des paiements anonymes grâce au concept de la signature aveugle : le numéro de série d'une pièce électronique est combiné avec un facteur d'aveuglement, avec lequel ce numéro sera multiplié arithmétiquement.

Pour les paiements, même si plusieurs systèmes ont été proposés récemment, seul *MilliCent*, mis au point par la Société *Digital*, a dépassé la phase de recherche. Aujourd'hui en phase de tests, il permet le paiement de montants de quelques centimes à l'aide de coupons émis par chaque commerçant ou gérés au préalable de courtiers virtuels.

Transactions généralisées

En analysant tous ces systèmes, nous avons déterminé les besoins à combler. Nous avons alors proposé un nouveau système de paiement, qui généralise le concept de valeurs numériques sans restrictions sur leur nature intrinsèque.

Bien qu'ils varient par la manière dont ils effectuent une transaction, tous les systèmes actuels ne font qu'une seule opération : un paiement électronique. Pour étendre cette fonction, nous avons mis au point le système *TRANZIX*, qui ouvre la porte à toute autre transaction, tels le transport, le transfert ou l'échange de valeurs. La notion de valeur généralise le concept de paiement.



2. AVANT UN PAIEMENT À L'AIDE DE TRANZIX, l'acheteur achète de l'argent numérique. L'acheteur clique sur un lien dans un magasin virtuel. Le serveur virtuel du vendeur contacte alors celui de l'acheteur en envoyant une requête de paiement pour la marchandise demandée. Lorsque le paiement est approuvé par l'acheteur, le vendeur reçoit un ou plusieurs billets numériques qu'il peut déposer immédiatement à la banque afin de vérifier leur validité, prévenant ainsi toute tentative de dépenses multiples. Le vendeur peut faire les vérifications hors ligne (les flèches vertes représentent des transactions qui se font en ligne ou hors ligne ; les flèches rouges représentent des transactions hors ligne et les flèches noires des transactions en ligne).

Est-ce risqué d'acheter en ligne ?

Est-il plus risqué d'acheter sur l'Internet que de faire un achat par Miniel ou par téléphone ? Lorsque l'on achète sur l'Internet, le site propose en général plusieurs options.

Si le site n'est pas sécurisé (le navigateur prévient l'internaute lorsqu'il passe sur un site sécurisé), on vous proposera le plus souvent d'imprimer le bon de commande et de l'envoyer par fax ou par la poste ce qui revient à un achat par correspondance, dont on ne discutera pas la sécurité.

Parfois on vous proposera d'entrer votre numéro de carte de crédit en clair. Évitez de le faire, car même si, à l'instar du téléphone, tout le monde n'est pas sur écoute, il existe de logiciels conçus pour enregistrer les messages qui transitent sur le réseau et qui repèrent les suites de 16 chiffres, tels les numéros de carte de crédit. Ainsi, on a saisi des listes de millions de numéros de cartes de crédit chez des pirates américains.

Lorsque le site est sécurisé, le chiffrement dépend du lieu de la boutique et de l'endroit où vous êtes. S'il s'agit d'une boutique américaine, telle la librairie en ligne Amazon.com, la sécurisation théorique est SSL 128 bits. Toutefois, si vous êtes en France, le navigateur que vous utilisez sera bridé en 40 bits, le temps que les navigateurs acceptant plus apparaissent, ou en 56 bits, car, jusqu'à présent, le gouvernement américain refusait l'exportation de

logiciels de cryptographie avec une clé secrète plus longue que 56 bits. Si la boutique est en France, vous aurez vraisemblablement affaire à un chiffrement SSL 40 bits.

Le chiffement SSL avec une clé de 40 bits est-il sûr ? En juillet 1994, un informaticien lança un défi : pouvait-on facilement percer un message chiffré par ce système. Un informaticien français, Damien Doligez, de l'Institut national de recherche en informatique et automatique (INRIA), explora toutes les clés possibles et décrypta le message après huit jours de calculs sur différents ordinateurs dont il disposait, dont des machines parallèles. Aujourd'hui, la vitesse de calcul des ordinateurs a considérablement cru et on obtiendrait le même résultat avec des ordinateurs à base de *Pentium* (PC) ou de

Pentium Pro (Mac), facilement disponibles. Cela signifie-t-il qu'il faut avoir peur de mettre son numéro de carte de crédit en ligne ? Le risque est faible, car quel pirate passerait des jours à decrypter un message pour obtenir un numéro de carte de crédit alors que des factures et des cartes de crédit traînent dans les magasins ?

Quand les systèmes de cryptographie avec des clés secrètes de 128 bits seront disponibles en France et en Europe, ce risque minime n'existera plus : même avec les ordinateurs les plus puissants au monde, des messages chiffrés à l'aide de systèmes tels que PGP nécessiteraient des années pour être percés.

Ainsi, pour *TRANZIX*, la notion de valeur représente tout objet virtuel ayant une valeur non intrinsèque quelconque, donc tout document numérique valant quelque chose pour quelqu'un. Ces documents incluent les billets virtuels, les certificats numériques, les attestations électroniques (diplômes d'études, preuves d'achat ou de vente, etc.), les moyens d'identification (carte santé, permis de conduire, passeport, etc.)...

TRANZIX généralise non seulement la notion de valeur, mais aussi l'opération de paiement. Ainsi, une valeur peut être transférée de A à B, de B à C, de C à D, etc. ; elle peut être échangée de possesseur. Elle peut être transférée de B à C, non seulement en changeant d'endroit – par transport –, mais en changeant aussi de possesseur. Enfin, elle peut être échangée, lors d'une même transaction, contre d'autres valeurs ; la notion d'échange implique donc deux transferts, lors d'une même transaction. Par exemple, *TRANZIX* permet à un usager de transporter une autorisation électronique de chez lui à son bureau, de transférer cette autorisation à son employé afin d'ouvrir une porte ou d'accéder à une imprimante.

Le système assure un niveau de sécurité très élevé, obtenu grâce à un chiffement asymétrique (deux clés de chiffement complémentaires sont utilisées ; voir *Cryptographie et réseau*, page 38). De surcroît, la granularité est réglable. C'est une solution exclusivement logicielle, où les utilisateurs peuvent acheter ou vendre en ligne ou hors ligne à l'aide d'un même portefeuille virtuel.

En pratique, comment s'effectue une transaction ? Après avoir acheté des billets numériques, l'acheteur active son portefeuille virtuel en suivant un lien hypertexte payant dans un magasin virtuel. Le portefeuille virtuel du vendeur contacte alors celui de l'acheteur en lui envoyant une requête de paiement pour la marchandise demandée (voir la figure 2). Une fois le paiement approuvé par l'acheteur, un ou plusieurs billets numériques sont envoyés au vendeur, qui peut les déposer immédiatement dans son portefeuille virtuel, évitant ainsi toute tentative de dépenses multiples.

Le vendeur peut aussi choisir d'effectuer des transactions hors ligne, afin d'augmenter la vitesse de traitement pour les microtransactions, par exemple ; les billets sont alors déposés par lots à la banque à la fin de la journée ou de la semaine. De cette manière, en réduisant les coûts de traitement des transactions, *TRANZIX* rend économiquement viables les microtransactions.

Tout comme dans le monde réel, où plusieurs systèmes de paiement coexistent, plusieurs moyens de paiement numériques seront présents dans le portefeuille virtuel du consommateur de demain. En définitive, les consommateurs décideront quels moyens transactionnels répondent le mieux à leurs besoins spécifiques et quels types de systèmes particuliers survivront dans l'économie virtuelle du futur.

Octavien URECHE prépare sa thèse de doctorat au laboratoire SCIBENS de l'École polytechnique de Montréal dont Réjean PLAMONDON est le directeur.

O. URECHE et R. PLAMONDON, *Document Transport, Transfer and Exchange : Security and Commercial Aspects*, 5th International Conference on Document Analysis and Recognition, in *IEEE Computer Society*, Bangalore, 1999.

O. URECHE et R. PLAMONDON, *Système électronique de transfert numérique de valeur : étude de faisabilité*, École polytechnique de Montréal, EPM/RT-96/22, 1996.

Pour la libéralisation de la cryptographie

RONALD RIVEST

L'un des pionniers de la sécurité informatique s'oppose au contrôle gouvernemental de la cryptographie.

Le développement de la cryptographie est une conséquence inéluctable de la révolution informatique. Avec l'apparition des communications entre les ordinateurs, les utilisateurs cherchent à sécuriser les conversations et les transactions. La cryptographie est la... clé de cette sécurisation, mais sa généralisation est débattue. Aux États-Unis, le gouvernement veut restreindre l'usage de la cryptographie ; les espions ne l'utilisent.

Avant 1970, la cryptographie était trop compliquée et trop onéreuse pour un usage courant. Grâce à deux inventions – la cryptographie à clé publique et le microprocesseur –, les méthodes cryptographiques sont devenues si performantes qu'il faudrait des années de calcul sur ordinateur pour décoder un message dont on ignore la clé. Les ordinateurs capables d'exécuter ces méthodes sont devenus largement accessibles.

Toutefois, vers la fin des années 1980, lorsqu'une cryptographie civile devint ainsi possible, deux agences américaines s'inquiétèrent de sa généralisation. L'Agence de sécurité américaine (NSA, soit *National Security Agency*), qui surveille les communications électroniques mondiales, s'alarma de ne plus pouvoir décrypter les messages chiffrés d'espions ou de terroristes potentiels.

D'autre part, les criminels utilisent de logiciels de cryptographie pour déjouer la surveillance de leurs communications. Durant la dernière décennie, ces organismes ont poussé le gouvernement américain à réglementer l'usage de la cryptographie et à limiter l'exportation de logiciels de cryptographie.

Doit-on priver l'ensemble des utilisateurs de techniques, sous prétexte que quelques criminels pourraient les utiliser à leur avantage ? L'argument est spécieux : on n'empêche pas le public d'acheter des gants sous prétexte que les voleurs en utilisent pour éviter de laisser des empreintes digitales. Restons sur ce dernier exemple.

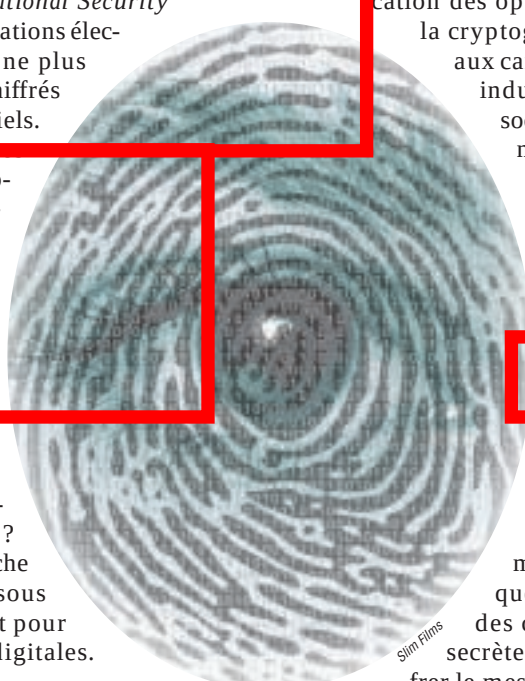
La cryptographie protège les données ; les gants protègent les mains. Les gants protègent les données et les espions industriels ; les gants protègent contre les coupures, la chaleur, le froid et les infections. La cryptographie peut gêner la police, qui ne pourra plus pratiquer d'écoutes téléphoniques ; les gants peuvent gêner la police qui trouve difficilement des empreintes digitales. La cryptographie est difficile à utiliser et d'emploi difficile ; les gants le sont depuis longtemps. Enfin, on peut télécharger des logiciels de cryptographie à partir du réseau Internet pour un coût inférieur à celui d'une bonne paire de gants.

Le travail de la police deviendra certainement plus difficile si tous les utilisateurs du réseau chiffrent leurs échanges, mais nous ne sortirons correctement de ce dilemme que si nous pesons les avantages et les inconvénients collectifs de l'innovation. La plupart des utilisateurs envisagent d'utiliser la cryptographie pour prévenir les crimes plutôt que pour protéger leurs données.

En assurant la confidentialité et l'authentification des opérations bancaires et commerciales, la cryptographie empêche le vol et la fraude aux cartes de crédit, et elle évite le piratage industriel. Paradoxalement, on créera une société plus sûre si l'on adopte une technique qui entrave quelque peu l'application des lois.

Certains ont souhaité un compromis qui généraliserait les systèmes cryptographiques élaborés en permettant aux États de déchiffrer les messages en cas de besoin : par exemple, on pourrait demander aux États de garder une clé secrète.

On a aussi proposé de donner aux autorités des moyens secrets d'accéder à ces clés. Une version cryptée de la clé qui a chiffré le message serait envoyée en même temps que celui-ci. Un centre de recouvrement des clés pourrait utiliser une super clé secrète pour déchiffrer la clé, puis déchiffrer le message lui-même.



La réglementation en France

Pendant longtemps, la cryptographie a été considérée comme une arme ; son usage était réglementé, aussi bien pour la fourniture et l'exportation que pour l'utilisation à titre privé.

En février 1998, toutefois, l'État français a autorisé tout procédé nécessaire à l'authentification de données ou d'entités (intégrité, signature numérique et contrôle d'accès), ainsi que le chiffrement des communications, en limitant, dans ce dernier cas, la clé secrète à 40 bits. Une telle taille de clé est jugée suffisante pour des applications «sérieuses» : à raison d'un million d'essais par seconde, une station de travail trouve la clé en moins de 15 jours.

Comment accroître la sécurité ? En augmentant la taille de la clé et en déposant alors la clé secrète auprès d'un tiers de confiance. Ce dépôt permettait alors aux instances judiciaires d'obtenir, de ce tiers de confiance, la clé secrète nécessaire au déchiffrement de communications chiffrées, en cas de besoin.

Le 19 janvier 1999, le premier ministre, Lionel Jospin, annonçait une proche libéralisation de l'usage de la cryptographie. Après avoir interrogé les acteurs, les experts et les partenaires internationaux, le gouvernement a retenu les orientations suivantes : libéraliser complètement la cryptographie ; supprimer le recours obligatoire aux tiers de confiance pour le dépôt des clés secrètes de chiffrement ; compléter le dispositif juridique afin d'obliger la remise aux autorités judiciaires de la

transcription en clair des documents chiffrés, lors de leur demande. De telles modifications législatives nécessiteront plusieurs mois.

Pour lever rapidement les principales entraves au développement du commerce électronique et pour assurer la confidentialité des communications, des décrets, parus le 10 mars 1999, relèvent le seuil de la cryptographie libre. Plus précisément, ces décrets stipulent que «les matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clé est d'une longueur inférieure ou égale à 40 bits sont totalement libres» et que «les matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clé est d'une longueur supérieure à 40 bits et inférieure ou égale à 128 bits sont libres sans condition pour un usage privé, et soumis à déclaration dans les autres cas».

Ces décrets ont été publiés dans le *Journal Officiel* le 10 mars 1999.

La libéralisation de la cryptographie pose cependant une question importante : une attaque par recherche exhaustive (essai de toutes les clés) nécessiterait plusieurs siècles, même avec tous les ordinateurs de la planète réunis. Une autre étape importante, sera «d'assurer, avec toutes les garanties nécessaires, la valeur probante du document sous forme numérique et des signatures électroniques. Les obstacles juridiques qui demeurent au développement des transactions dématérialisées seront ainsi levés».

David POINTCHEVAL, École normale supérieure, Paris

Ces systèmes ne satisferont personne, car ils sont faciles à détourner. Les logiciels de chiffrement pour empêcher la recherche de la clé ou utiliser d'autres logiciels disponibles sur le réseau Internet. De surcroît, avec ces solutions, la recherche des clés serait très onéreuse et le coût du recouvrement des clés n'a pas été envisagé : qui paiera ? Enfin, la confiance dans le gouvernement risquerait de s'éroder, et la procédure serait très compliquée : imaginez qu'à chaque achat de gants vous soyez légalement tenus de coudre des copies en latex de vos empreintes digitales aux doigts de ces gants !

Les systèmes de recouvrement de clés seraient également dangereux. La procédure secrète utilisée par le FBI pour déchiffrer les messages pourrait être détournée au profit de criminels, d'intrus, d'espions ou même d'employés mécontents du FBI. En volant une super clé secrète, ces indélégats pourraient déchiffrer les messages secrets appartenant à des sociétés, à des personnes privées ou au gouvernement seraient brusquement vulnérables.

En 1998, la Commission nationale de l'informatique et des libertés a étudié ces problèmes. Après deux années de travail, la commission a conclu pour l'occasion à l'estime que la libéralisation de la cryptographie était plus avantageuse que son interdiction. Aucune loi ne devrait limiter la fabrication, la vente et l'utilisation des systèmes cryptographiques à l'intérieur des États-Unis.

Les membres de la commission ont également estimé que l'État ne pourrait pas faire respecter une interdiction de la cryptographie. Pourtant, le FBI et la NSA prônent tou-

jours la mise en place d'un service de recouvrement des clés. Ils s'opposent au relâchement des contrôles à l'exportation, tant que la possibilité de retrouver les clés secrètes n'est pas assurée.

Entre-temps, la cryptographie s'est développée, les utilisateurs se sont familiarisés avec les programmes de cryptographie, et le contrôle deviendra inéluctablement difficile. Les entreprises adoptent des standards publics de cryptographie que même des lycéens peuvent convertir en programmes. De surcroît, il existe de nouvelles techniques qui ne chiffrent pas le message, mais permettent la confidentialité des communications en utilisant des clés aléatoires. D'où la difficulté d'un contrôle !

Je maintiens que les citoyens doivent avoir le droit d'avoir des conversations privées. La démocratie repose sur la possibilité que possède chaque citoyen de partager librement ses opinions de voir, sans crainte de surveillance ou de représailles. Ce principe doit être appliqué au «cyberespace», comme il l'est au monde réel. Si les États-Unis restreignent le droit d'utiliser la cryptographie, ce serait un recul de la démocratie et une victoire de *Big Brother*.

Donald RIVEST est l'un des inventeurs de la méthode de chiffrement RSA. Il enseigne à l'Institut de technologie du Massachusetts.

Whitfield DIFFIE et Susan LANDAU, *Privacy on the Line : The Politics of Wiretapping and Encryption*, MIT Press, 1998.

Les galets, outils du Paléolithique

SOPHIE A. DE BEAUNE

Des galets non taillés révèlent l'invention de gestes techniques avant la fabrication d'outils spécialisés.

Les silex taillés sont parmi les vestiges les plus impressionnants et les plus abondants laissés par les hommes du Paléolithique. Les images et les récits ont popularisé la vision de l'«homme des cavernes» taillant un silex ou le brandissant pour chasser. C'est aussi par la typologie de cet outillage, le «silex taillé», que les grands ensembles culturels ont été définis : l'Aurignacien, le Gravettien, le Solutréen, le Magdalénien...

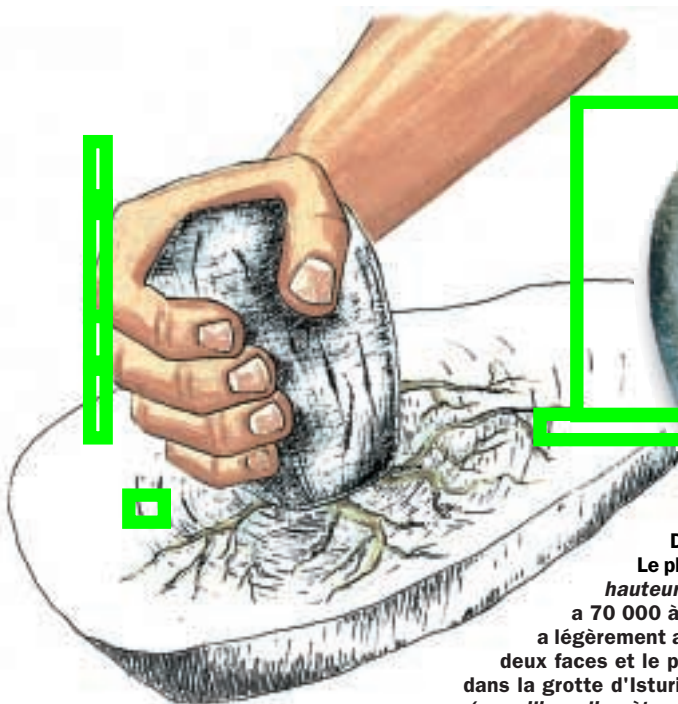
Toutefois, nos ancêtres ne taillaient pas la pierre plus que nécessaire : pour la plupart des outils en roche non cassante utilisés pour leurs besoins domestiques et techniques courants, ils

ménageaient leur peine et choisissaient des blocs, des plaquettes ou des galets dont la forme naturelle était proche de ce qu'ils recherchaient. Ainsi, pour obtenir des récipients en roche dure, ils ramassaient des galets ronds ou ovales, dont ils n'avaient plus qu'à creuser l'une des faces. Ils utilisaient aussi qu'ils aient la taille, la forme, la dureté et la densité voulues. Ils en faisaient alors des enclumes, des broyeurs, des molettes, des pilons-broyeurs, des maillets, des lissoirs, des polissoirs... Bien que rudimentaires, ces outils étaient conservés et exploités très longtemps.

Ces outils «naturels», ou façonnés par des techniques autres que la taille

(piquetage, martelage, raclage, plus rarement polissage), ont été longtemps négligés. Les préhistoriens du XIX^e siècle et de la première moitié du XX^e siècle les abandonnaient souvent dans les inventaires de déblais. Dans le meilleur des cas, ils les conservaient sous une rubrique «divers».

Heureusement, quelques sites font exception, telles les grottes pyrénéennes de La Vache, fouillée de 1866 à 1940, et d'Isturitz, de 1912 à 1954, dont l'intégralité du matériel a été conservée : les galets utilisés y sont si abondants (presque 500 pour chaque site) que leur



1. DES MOLETTES, ou meules à main, étaient utilisées pour le broyage, de végétaux par exemple, par un mouvement de bascule d'avant en arrière et de droite à gauche.

De nombreuses formes naturelles des galets se prêtent à cet usage. Le plus ancien témoignage en est un galet de roche volcanique (à droite, hauteur réelle : 7,5 centimètres), manipulé par des Néandertaliens il y a 70 000 à 40 000 ans dans le Petit Abri de Laussel, en Dordogne. L'usage a légèrement aplati sa face inférieure. De même, le frottement répété a poli les deux faces et le pourtour d'un petit galet de quartzite quasi circulaire, découvert dans la grotte d'Isturitz, dans les Pyrénées-Atlantiques, et daté de 28 000 à 22 000 ans (au milieu, diamètre réel : 6,5 centimètres).

classement, respectivement par Dominique Buisson, alors au Musée des antiquités nationales, et par moi-même, a permis de constituer des collections utilisables pour des comparaisons au fur et à mesure des nouvelles découvertes. Aujourd'hui, les fouilleurs récupèrent l'intégralité du matériel archéologique.

Cet outillage, que l'on retrouve sous des formes analogues chez des peuples nomades actuels, chasseurs-cueilleurs ou éleveurs, nous renseigne sur la vie quotidienne de leurs utilisateurs. Très variés, ces outils sont intervenus aussi bien dans la transformation de la matière que dans la consommation et l'acquisition de la nourriture : fabrication de l'outillage, préparation de la nourriture, stockage de divers ingrédients, préparation des colorants, éclairage, travail des peaux, chasse, pêche...

Les traces d'utilisation visibles à la surface de ces objets permettent la reconstitution des gestes exécutés. Notre connaissance des activités et des comportements des hommes du Paléolithique en est élargie. Par exemple, au Roc de Sers, en Charente, un bloc ayant servi à la fois d'enclume pour débiter du silex et de support de vêtements de peaux apporte de nombreuses informations sur la taille de la pierre, mais aussi sur les techniques de découpe et de préparation alimentaire, et sur la gestion de l'espace dans le campement. Les galets non taillés nous informent aussi sur la consommation et les modes de préparation des végétaux sauvages, dont presque toutes les traces

directes ont aujourd'hui disparu (les restes végétaux se fossilisent mal). Sur tout, nous savons que l'étude des gestes auxquels sont liés ces outils pose de façon nouvelle la question du progrès, du début du Paléolithique au Néolithique : de nombreuses innovations techniques résultent de la simple application de gestes anciens à un nouveau but.

Des traces à la fonction

À quelles activités les traces que nous observons sur les objets préhistoriques répondent-elles? Comment pourrions-nous déterminer si elles ont été produites par la seule utilisation de l'objet ou au cours d'une éventuelle fabrication? Dans un premier temps, nous devons retrouver le fonctionnement de ces objets : comment ont-ils été utilisés? Nous pourrions ensuite formuler des hypothèses sur leurs fonctions.

En 1943, André Leroi-Gourhan a proposé une classification des « moyens élémentaires de l'industrie humaine », qui lui a servi de base pour une classification générale de l'ensemble des techniques humaines. Sa classification des percussions suffit pour tenter d'élucider l'origine des traces visibles sur les galets préhistoriques. J'ai ainsi obtenu quatre grandes catégories d'outils, actifs ou passifs : ceux ayant exercé ou subi une percussion lancée, ceux ayant exercé

ou subi une percussion posée, ceux ayant alterné une percussion lancée et posée, enfin ceux n'ayant reçu ou exercé aucune percussion. Cette terminologie ne résume pas de la nature de l'activité réalisée et se limite à la description d'un geste.

J'ai ensuite défini des critères qui permettent de dire comment le geste s'est exercé. Pour cela, je tiens compte du type de support (galet ou bloc) et de l'emplacement des traces d'usage par rapport à la forme de l'objet (sur la face, sur le flanc, sur la tranche, concentrées ou éparées) pour en déterminer la spécificité. D'autres paramètres, tels la nature et les caractéristiques de la roche, facilitent le diagnostic. Cette méthode s'appuie sur plusieurs méthodes : la tracéologie, mais aussi l'expérimentation, la confrontation avec les vestiges voisins et l'observation ethnographique.

Lorsque nous avons ainsi retrouvé le fonctionnement d'un galet, nous nous intéresser à sa fonction, en remplaçant les gestes au sein d'une chaîne opératoire : par exemple, pour



2. LA MOULURE était connue de certains groupes du Paléolithique, bien avant l'invention de l'agriculture. Les stries et les traces de colorant visibles sur la surface de cette grande plaque de schiste (en bas, longueur réelle : 28 centimètres) qui provient de l'abri du Cap Blanc, en Dordogne, attestent en effet que de l'argile a été broyée et moulue, il y a 14 000 à 11 000 ans. C'est l'une des rares meules entières connues au Paléolithique supérieur. Elle a été utilisée avec un broyeur semblable à ce volumineux galet de grès rose (en haut, longueur réelle : 13,5 centimètres), dont les faces et les flancs sont usés et striés. Celui-ci, qui provient de niveaux de 28 000 à 22 000 ans de la grotte d'Isturitz, dans les Pyrénées-Atlantiques, a fait l'objet d'un ravinage de ses surfaces, comme cela se pratiquait fréquemment à partir du Néolithique : la surface est piquetée pour être rendue à nouveau rugueuse, afin de mieux mordre la matière à moudre et à écraser.

préparer la peau (l'activité), il faut la gratter, donc exercer une pression sur sa surface (l'action) en une série de gestes (l'effort physique) à un stade, tous les outils possibles ne sont jamais certains. Ainsi, bien que nous ne soyons pas sûrs qu'elles en pierre ont été utilisées par percussion indirecte légère (on a tapé dessus avec un percuteur), nous ne saurons sans doute jamais avec certitude s'il a servi à sculpter des objets en bois de cervidé ou en ivoire de mammouth.

La boîte à outils

Dans certains cas, les traces d'usage laissent supposer que l'outil était réservé à une seule fonction. Elles sont en outre parfois si nettes, si caractéristiques, que l'on reconnaît sans embarras cette fonction : petites molettes circulaires à une main (voir la figure 1), broyeurs allongés, galets volumineux à surfaces planes ou légèrement creusées ayant

servi de meules (voir la figure 2). On est souvent aidé par la comparaison avec l'outillage encore existant dans certaines sociétés, tel le matériel de broyage et de mouture de Tichitt, en Mauritanie (voir la figure 3), ou de la Préhistoire et technologie du CNRS.

À l'inverse, la fonction d'autres objets n'a pas encore été élucidée. Ainsi les cupules que portent certains galets et certains blocs révèlent-elles que ces objets ont servi en percussion lancée, mais possédaient-ils en position active ou passive (voir la figure 3).

À côté de ces outils spécialisés, de nombreux autres ont servi à de multiples tâches. Ils présentent, sur tout ou partie de leur surface, les stigmates de trois ou quatre usages différents, voire davantage. Pour des objets souvent petits et portatifs, on peut envisager un usage actif mobile et un usage passif, où l'objet est maintenu immobile dans le creux de la main ou coincé entre les pieds.

Les exemples contemporains d'outils plurifonctionnels et utilisables indifféremment en position active ou passive ne manquent pas. Ainsi, il y a quelques années, j'ai observé les utilisateurs d'un galet de quartz dans un campement touareg kel-ferwan de la région d'Agadez, au Niger (voir la figure 4). Cet objet porte des traces de piquetage, le long de ses arêtes longitudinales et au centre d'une de ses faces. Les deux facettes de la face opposée ont été produites par usure. Il est maculé de nombreuses traces noires : charbon à l'une des extrémités, colorant sur une des facettes et sur l'autre extrémité des traces de pulpe de fruit sur l'autre face.

Chaque type de trace correspond à un usage spécifique. Ce galet était d'abord utilisé pour le piquetage, au lissage du cuir, mais il servait aussi, à l'occasion, de support pour écraser la pulpe du fruit oléagineux ou pour briser des pains de sucre, de broyeur pour écraser des herbes médicinales, du charbon de bois ou du khôl, de marteau pour repousser du cuir avec un burin de fer.

La diversification des usages

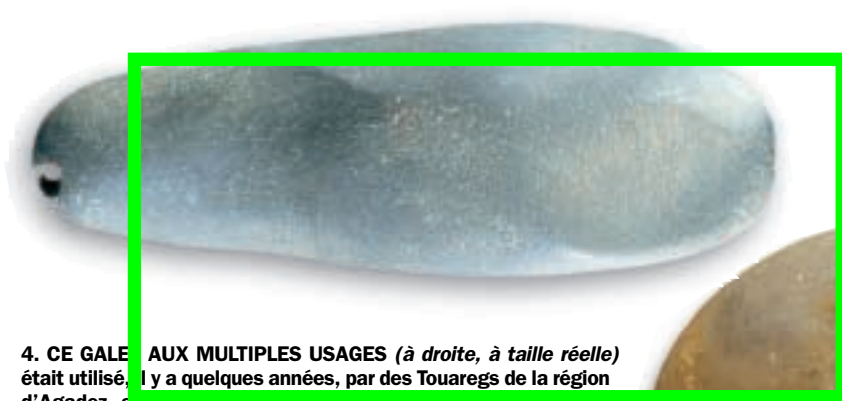
Il y a 2,6 millions d'années, des hominidés, australopithèques ou premiers représentants du genre *Homo*, utilisent déjà des galets et des éclats taillés que nous connaissons sont des galets et des éclats dont une pointe ou un tranchant ont été dégagés par des enlèvements de matière intentionnels. Ils sont utilisés pour découper le gibier, couper de la viande ou concasser des os afin d'en extraire la moelle comme en témoignent les traces qui subsistent sur ces derniers.

À côté de ce très ancien outillage taillé, d'autres outils sont fabriqués, quels qu'ils soient, comme enclumes ou comme marteaux pour casser, écraser ou faire éclater. Une partie de leur surface, ou l'une des extrémités porte des traces d'impacts et d'écrasements. Ils sont analogues aux galets utilisés aujourd'hui par certains chimpanzés pour concasser des coquilles de fruits durs.

L'utilisation des galets non taillés ne se diversifie qu'à partir du Paléolithique moyen, il y a 180 000 ans. On trouve alors les premiers galets



3. LA CUPULE CENTRALE de ce galet globuleux (taille réelle) témoigne de frappes répétées à cet endroit. Il a peut-être servi à casser des noix, dans la grotte d'Isturitz, dans les Pyrénées-Atlantiques, il y a 29 000 à 22 000 ans. Ce type d'outil non fabriqué est très répandu tout au long de la Préhistoire : les plus anciens ont environ 2,5 millions d'années et ont été utilisés par des australopithèques ou par les premiers représentants du genre *Homo*. En outre, certains groupes de chimpanzés cassent aujourd'hui des noix avec des percuteurs et des enclumes analogues. On ne peut toutefois exclure d'autres usages, comme maillet par exemple.



4. CE GALET AUX MULTIPLES USAGES (à droite, à taille réelle) était utilisé, il y a quelques années, par des Touaregs de la région d'Agadez, au Niger. Il porte des traces associées à plusieurs activités, domestiques, médicinales, artisanales, voire ludiques.

Cet outil à l'usage multiple a une grande valeur puisqu'il est soigneusement conservé toute la vie et transmis de mère en fille : un outil « brut » n'est donc pas moins précieux qu'un outil façonné. De tels galets, analogues au couteau suisse que l'on porte toujours sur soi, étaient aussi employés au Paléolithique : par exemple un galet magdalénien (il y a 15 000 à 12 000 ans) en schiste, découvert dans la grotte de l'Église à Excideuil, en Dordogne (en haut, longueur réelle : 15,2 centimètres). Il porte des traces d'impact et des facettes pour une usure correspondant à des usages comme percuteur, broyeur et enclume. La perforation permettait de le suspendre avec un lien.

présentant, en plus des traces d'écrasement ou de piqueté, des plages polies par frottement. On peut imaginer qu'il effectuait une action de broyage. Cette diversification des traces atteste une diversification des activités : au concassage de fruits durs et d'os, s'ajoute la préparation et la régularisation de surfaces ou encore le broyage de substances végétales ou animales en vue de leur consommation (glands, racines, viande, graisse...).

Au Paléolithique supérieur, qui débute il y a 40 000 ans, l'utilisation des galets s'intensifie. De l'Aurignacien au Magdalénien supérieur (de 40 000 à 10 000 ans), cet outillage sur bloc ou sur galet devient de plus en plus fréquent, et il se diversifie, tant pour la matière première que pour les formes et la nature des traces d'usage, ce qui correspondrait à une spécialisation de plus en plus poussée. On trouve pour cette période des galets lustrés sur un bord ou sur une face et exempts de stries, sans doute des lisseurs pour aplanner les peaux et les cuirs. De petits blocs de grès couverts de rainures étaient destinés à régulariser et à polir.

les sagaies en os (voir la figure 7). De petits galets à grain fin, de forme arrondie, ont servi de martelets pour façonner, par percussion sur un burin ou un ciseau, des objets en matière dure animale, os, ivoire ou bois de cervidé.

Au matériel de concassage qui existait déjà, vient s'ajouter un outillage plus spécifiquement destiné à broyer

TEMPS ÉCOULÉ (EN ANNÉES)	TRACES ET IMPACTS	FONCTIONS
260 000	IMPACTS, CUPULES TRACES D'ÉCRASEMENT	TAILLE DE LA PIERRE CONCASSAGE D'OS ET DE NOIX
180 000	STRIES PLAGES LUSSES	BROYAGE PRÉPARATION DE SUBSTANCES
40 000	TRACES DE COLORANT	BROYAGE DE COLORANT
29 000	LUSTRAGE, POLI ÉCRASEMENT	LISSAGE DE PEAUX PILAGE, BROYAGE
17 000	RAINURES	POLISSAGE D'OBJETS EN OS
10 000	RÉSIDUS VÉGÉTAUX MORTIERS ET PILONS FAÇONNÉS MEULES FAÇONNÉES	MOUTURE DE VÉGÉTAUX SAUVAGES MOUTURE DE CÉRÉALES

5. L'usage des galets non façonnés est très ancien, mais les fonctions (dédiées en particulier des traces d'usage) n'ont commencé à se diversifier qu'il y a 40 000 ans. Certains de ces objets, notamment les instruments de broyage, sont les ancêtres directs d'outils plus élaborés tels les pilons, les mortiers et les meules en pierre fabriqués au Néolithique.

et à moudre différentes substances. Les premières meules et les premiers broyeurs datent du Châtelperronien, tout au début du Paléolithique supérieur, mais ils sont très rares. On trouve de nombreux blocs de grès destinés à réduire en poudre des blocs de colo-

Ce matériel se spécialise à partir du Châtelperronien, il y a 29 000 ans : meules planes ou légèrement concaves, meules-mortiers, molettes, broyeurs et pilons (voir la figure 8) portent des plages de poli d'usure associées ou non à de fines stries d'abrasion.

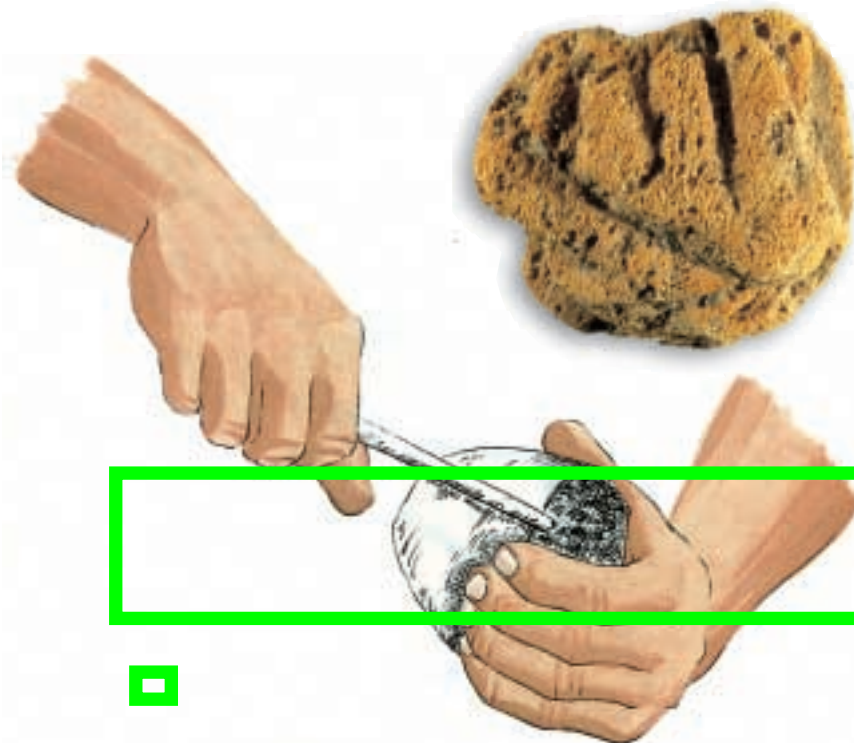
Presque tous ces outils de mouture présentent des traces de colorant : ou

bien les outils ayant servi à écraser d'autres matières, végétales ou animales, sont passés inaperçus à la fouille de ce qui serait surtout vrai pour les outils les plus anciens ; ou bien ils étaient effectivement destinés, au Néolithique, à moudre des substances

rares et ils n'ont été impliqués que progressivement dans des processus alimentaires. Une partie de cet outillage a toutefois servi pour le broyage de certaines graminées sauvages, de tubercules et même de fruits charnus, glands, noix ou noisettes. Ainsi, des résidus de tubéreuses de 19 000 à 17 000 ans ont-ils été trouvés à Wadi



6. LES TRACES D'IMPACT à la surface de ce pesant galet ovoïde en quartzite (*hauteur réelle : 10,5 centimètres*), surtout à ses extrémités, ainsi que son volume, sa forme et sa dureté indiquent qu'il était utilisé comme percuteur pour la taille et la retouche du silex, il y a 28 000 à 22 000 ans, dans la grotte de Pair-non-Pair, en Gironde.



7. LES RAINURES À SECTION EN U de 2,5 à 5 millimètres de profondeur et présentant des traces de polissage, à la surface de ce petit galet de pierre ponce (*taille réelle*), indiquent que des aiguilles en os ont été polies sur sa surface. C'est un objet assez rare. Il a en outre été ramassé, il y a 14 000 à 12 000 ans, sur le littoral (de l'Atlantique ou de la Méditerranée), à plusieurs dizaines de kilomètres de la grotte d'Isturitz, dans les Pyrénées-Atlantiques.

Kubbaniy, en Haute-Égypte, associés à du matériel de broyage.

Ce n'est toutefois qu'au Kébarien, il y a 17 000 à 12 000 ans au Proche-Orient, que le façonnage de ce type d'outillage se généralise : des mortiers et des pilons y sont pour la première fois entièrement sculptés, la plupart dans du basalte, et les mortiers sont creusés intentionnellement, contrairement aux mortiers du Paléolithique, qui ressemblent plus à des meules et dont le creusement est dû à l'usure. Ces objets sont surtout abondants à la période suivante, au Natoufien, où ils ont vraisemblablement servi au traitement des fruits sauvages, des glands, mais aussi des graines de céréales sauvages dont on a retrouvé des restes dans maints gisements. De même, bien que des meules aient existé dès le Paléolithique supérieur, les galets associés avec une forme asymétrique révélant une utilisation en un mouvement axial de va-et-vient, et qui sont ouvertes en deux pour faciliter la séparation du produit de mouture, n'apparaissent qu'avec les premières graines cultivées, à Mureybet et à Cheikh Hassan, en Syrie, il y a environ 10 000 ans.

Le geste précède la technique

Ces outils de broyage, apparus au début du Paléolithique supérieur, ont donc d'abord servi à autre chose qu'à la préparation des céréales. Les premiers indices de mouture de graines sauvages datent seulement de la fin de cette période : on a retrouvé des graines d'orge et d'avoine sauvages à Franchthi en Grèce, et dans d'autres sites du Levant. Rien ne permet toutefois d'affirmer que le broyage était répandu. Même les mortiers et les meules du Kébarien et du Natoufien, dont nous avons vu qu'ils sont plus élaborés techniquement que les outils de mouture magdaléniens qui leur étaient contemporains en Europe, préexistent à des gestes de broyage concernant d'autres matières, végétales, animales ou minérales.

Les gestes techniques du broyage sont donc antérieurs au Néolithique. Lorsque les hommes ont commencé à consommer des céréales sauvages, ils leur ont appliqué ces gestes, le broyage devenant alors mouture. Un transfert technologique semblable



8. LE PILAGE, par exemple de fruits, a été pratiqué avec ces deux galets, il y a 29 000 à 22 000 ans dans le Grand Abri de Laussel, en Dordogne. Celui du milieu (*taille réelle*) est en calcaire. Toutes ses faces ont été régularisées et sa base est aplanie par l'usage due aux écrasements répétés. Sa forme tronconique rappelle celle des pilons-battoirs polynésiens utilisés pour écraser la pulpe de certains fruits. Relativement rare, ce type d'outil est aussi attesté au Magdalénien (il y a 15 000 à 18 000 ans). Le galet en forme de rondin (*à droite, à taille réelle*) est en grès quartzitique. Sa pointe mousse (*en bas*), très usée, est lustrée et porte de légères traces d'impact, tandis que l'autre extrémité est émoussée et striée. Les encoches sur les flancs semblent être uniquement décoratives.

avait été réalisé pour les percuteurs, d'abord uniquement destinés au concassage, puis appliqués à l'obtention de pointes et de tranchants par l'éclatement de roches cassantes.

Ces deux exemples montrent que l'«invention» ou l'émergence d'un geste (ou d'une série de gestes mécaniques) précède celles de certaines des tâches auxquelles il peut servir. L'apprentissage, dès l'enfance, des connaissances techniques par imprégnation quotidienne serait, selon Gilbert Simondon, responsable d'une certaine rigidité, ces connaissances étant apprises sans être nécessairement pensées ou discutées et sans être remises en question. Éric Boëda, du laboratoire Préhistoire et technologie du CNRS, a ainsi remarqué la grande stabilité temporelle des techniques qui régissent le façonnage et le débitage du silex. Cette rigidité expliquerait en partie que toutes les applications possibles d'une habitude gestuelle ne sont pas d'emblée testées et adoptées.

Ainsi, toute activité nouvelle observée par les archéologues est le résultat de nouveaux gestes. Si les préhistoriens fondaient leurs conclusions sur les dates d'apparition effective des gestes, et non sur celles de leurs différentes applications, ou sur leur diffusion et de leur généralisation, ils n'obtiendraient vraisemblablement pas les mêmes découpages chronologiques et culturels que ceux qui sont en usage

actuellement. La distinction des civilisations est utile (la coupure entre le Néolithique et l'âge du fer est incontestable), mais des critères de distinction fondés sur la gestuelle, dans un esprit plus dynamique, plus fonctionnel, ne seraient-ils pas plus proches de la réalité que ceux fondés sur des différences d'outillage, d'ordre purement typologique?

Sophie A. de BEAUNE est chercheur au laboratoire d'ethnologie préhistorique du CNRS, Nanterre.

Sophie A. de BEAUNE, *Essai d'une classification typologique des galets et plaquettes utilisés au Paléolithique*, in *Gallia Préhistoire*, vol. 31, pp. 27-64, 1989.

K. WRIGHT, *The Origins and Development of Ground Stone Assemblages in Late Pleistocene Southwest Asia*, in *Paléorient*, vol. 17, n° 1, pp. 19-45, 1991.

André LEROI-GOURHAN, *L'homme et la matière*, Albin Michel, Paris, 1992.

Sophie A. de BEAUNE, *Les hommes au temps de Laussel, 40 000-10 000 avant J.-C.*, Hachette, Paris, 1995.

Sophie A. de BEAUNE, *Les galets utilisés au Paléolithique supérieur. Approche archéologique et expérimentale*, CNRS Éditions, Paris, 1997.

D. STORDEUR, *Néolithisation et outillage osseux. La révolution a-t-elle eu lieu?*, in *Préhistoire d'os*, recueil d'études offert à Henriette Camps-Fabrer, édité par M. Julien et al., Publications de l'Université de Provence, Aix-en-Provence et CTHS, Paris, à paraître.

Les cellules souches embryonnaires

ROGER PEDERSEN

Récemment isolées, ces cellules semblent capables d'engendrer la quasi-totalité des types de cellules de l'organisme. On envisage de les utiliser pour réparer les tissus et les organes endommagés.

Un randonneur a un infarctus en haute montagne. Le temps qu'il soit conduit à l'hôpital, le muscle cardiaque a été en grande partie détruit, faute d'oxygène. Aujourd'hui, le randonneur est condamné à une vie sédentaire. Demain, le malade pourra peut-être se rétablir : les médecins prélèveraient un petit lambeau de peau, extraient les cellules souches de ces cellules cutanées et l'injecteraient dans des œufs fécondés humains dont on aurait éliminé les chromosomes. Une culture de ces œufs modifiés conduirait à de tout jeunes embryons, auxquels on prélèverait ce que l'on nomme des cellules souches embryonnaires, capables de fabriquer différents types de cellules.

L'équipe médicale placerait ces cellules souches dans le cœur du malade dans des conditions telles qu'elles se différencieraient en cellules cardiaques compatibles avec les cellules du randonneur. Transplantées dans le cœur du malade, elles ne provoqueraient pas de rejet, s'y multiplieraient, remplaceraient les cellules détruites lors de l'infarctus, et le randonneur retrouverait santé et vigueur.

Ce scénario n'est plus invraisemblable. On connaît déjà plusieurs types de cellules souches. Les cellules souches embryonnaires sont capables d'assurer les fonctions de cellules du cœur, de foie ou de cerveau, mais dont les cellules filles se différencient, c'est-à-dire subissent des modifications telles qu'elles deviennent irréversiblement des cellules d'un type particulier. D'autres cellules filles restent des cellules souches : ainsi, des cellules souches

intestinales régénèrent sans cesse la paroi de l'intestin, des cellules souches cutanées fabriquent de la peau, et des cellules souches hématopoïétiques engendrent diverses catégories de cellules de sang. Chaque jour, nos cellules souches réparent les lésions et gèrent les usures subies par l'organisme.

Les cellules souches de l'embryon sont encore plus extraordinaires : elles peuvent engendrer tous les types de cellules de l'organisme. Pour la première fois, en 1998, des biologistes ont cultivé des cellules souches d'embryon humain. Ainsi, en février 1998, à l'Université du Wisconsin, James Thomson observe que certaines cellules humaines en culture ressemblent aux cellules souches qu'il avait précédemment obtenues à partir d'embryons de souris.

De là, à l'Université Johns Hopkins, John Gearhart isole des cellules analogues en cultivant des fragments d'ovaires et de testicules de fœtus humains. Simultanément, en Californie, des biologistes des Laboratoires Geron, à Menlo Park, et mes collègues, à l'Université de San Francisco, font des recherches similaires.

J. Thomson avait l'avantage d'avoir déjà travaillé sur les cellules souches de souris. Ses cellules de rat, de chien, de singe, de porc, de chèvre, de mouton, de rhésus et de quistitis. Au cours des mois qui suivirent, il réussit à déclencher la multiplication, en culture, de ces cellules fragiles, et il confirma qu'il s'agissait bien de cellules souches embryonnaires.

Dans un article publié dans la revue *Science*, le 6 novembre 1998, J. Thomson rapportait qu'une fois

transplantées sous la peau d'une souris ces cellules humaines forment divers tissus, par exemple de l'épithélium qui tapisse l'intestin, du cartilage, le os, des muscles ou encore de l'épithélium neuronal (le tissu précurseur du système nerveux). Ainsi, on obtient des structures issues des trois couches d'un embryon de mammifère : la couche la plus externe, l'ectoderme, la couche intermédiaire, le mésoderme, et la couche la plus interne, l'endoderme. Cette diversité est une preuve supplémentaire des potentialités de ces cellules, et les résultats obtenus laissent espérer que les recherches sur les cellules souches embryonnaires aboutiront un jour à la production de cellules utilisables pour le traitement de nombreux types de tissus.

Des possibilités illimitées

Si l'on avait commandé la différenciation de cellules souches embryonnaires en culture, on pourrait utiliser les cellules résultantes pour réparer les dégâts cellulaires causés par un arrêt cardiaque, par la maladie de Parkinson, par le diabète. Ces cellules seraient particulièrement utiles pour le remplacement des cellules cardiaques.

(détruits chez les personnes diabétiques), qui ne se renouvellent pas chez les adultes (le cœur et le pancréas ne renferment plus de cellules souches). Une découverte récente laisse envisager que l'on pourrait modifier des cellules souches déjà partiellement différenciées pour en reprogrammer le développement.

Avant que des cellules souches embryonnaires servent à des fins thérapeutiques, de nombreux problèmes devront encore être résolus. On devra, par exemple, déterminer la différenciation des cellules souches embryonnaires en un type de cellules spécifiques. L'essentiel de ce que l'on sait aujourd'hui en ce domaine est issu d'études menées sur des cellules

souches d'embryons de souris, les premières que l'on a isolées.

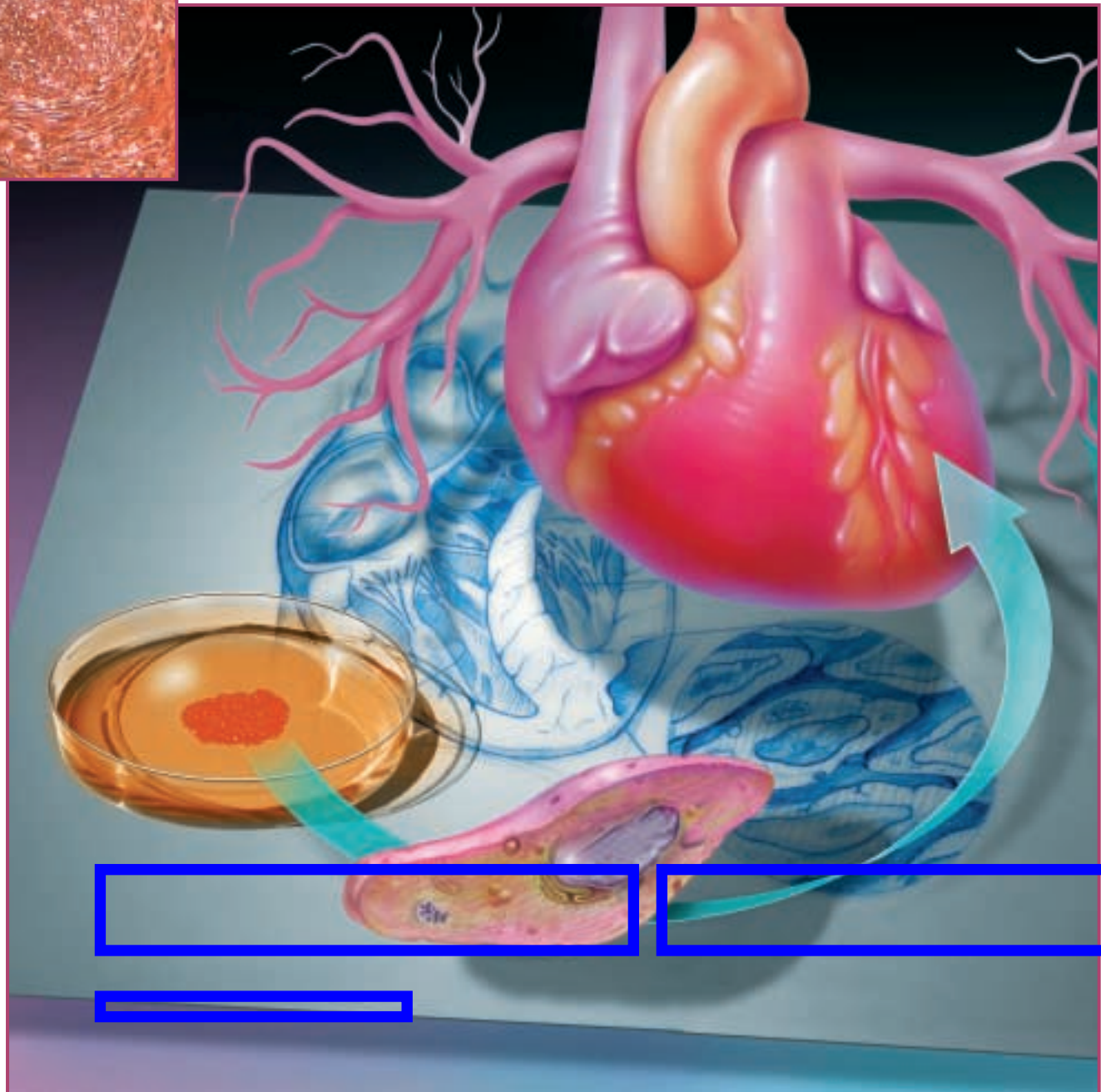
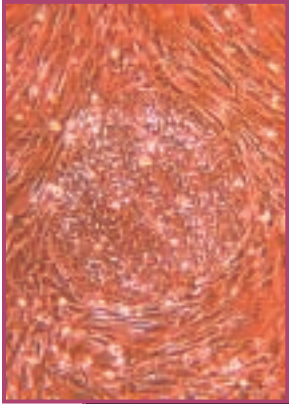
En 1981, des biologistes ont obtenu de telles cellules à partir d'embryons de souris.

Une certaine de cellules. Les embryons sont alors au stade blastocyste : ils forment une sphère creuse de cellules. La paroi interne d'un blastocyste – à peine plus large qu'un cil – présente un épaississement nommé masse cellulaire interne. Dans l'utérus, cette dernière formerait tout le fœtus, les membranes fœtales et l'amnios (la

membrane contenant l'embryon et le liquide amniotique).

Quand les blastocystes de souris sont cultivés dans une boîte de Pétri, les cellules souches embryonnaires et des cellules non différenciées de la masse cellulaire interne forment un

amas de cellules souches embryonnaires. Celles-ci se multiplient pendant longtemps, en restant indifférenciées. Pourtant, quand on les injecte dans un blastocyste de souris, elles réagissent à des stimulus physiologiques ; les cellules différenciées issues de ces cellules



1. LES CELLULES SOUCHES EMBRYONNAIRES humaines sont désormais obtenues en culture (l'amas central dans le cartouche du haut) ; dans cette boîte de culture, elles se sont développées sur une couche de cellules nourricières de souris. Les biologistes

envisagent de cultiver de telles cellules issues de tout jeunes embryons humains, afin de produire des cellules différenciées, voire des tissus, qui seraient utilisés pour la réparation d'organes endommagés, par exemple du cœur après un infarctus.

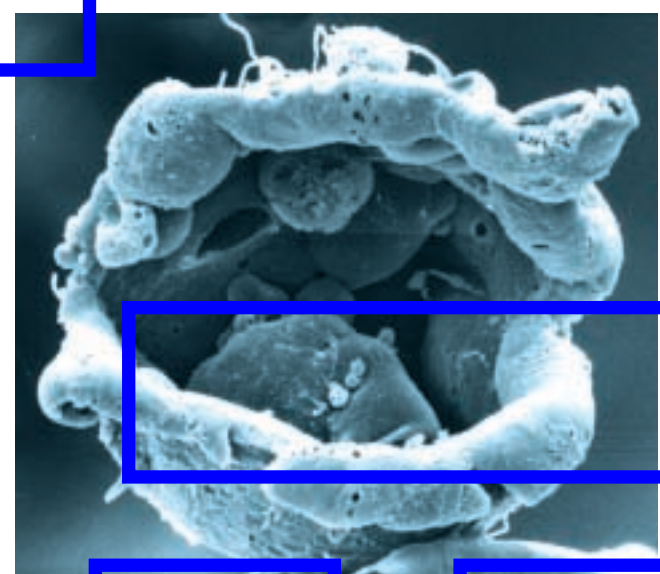
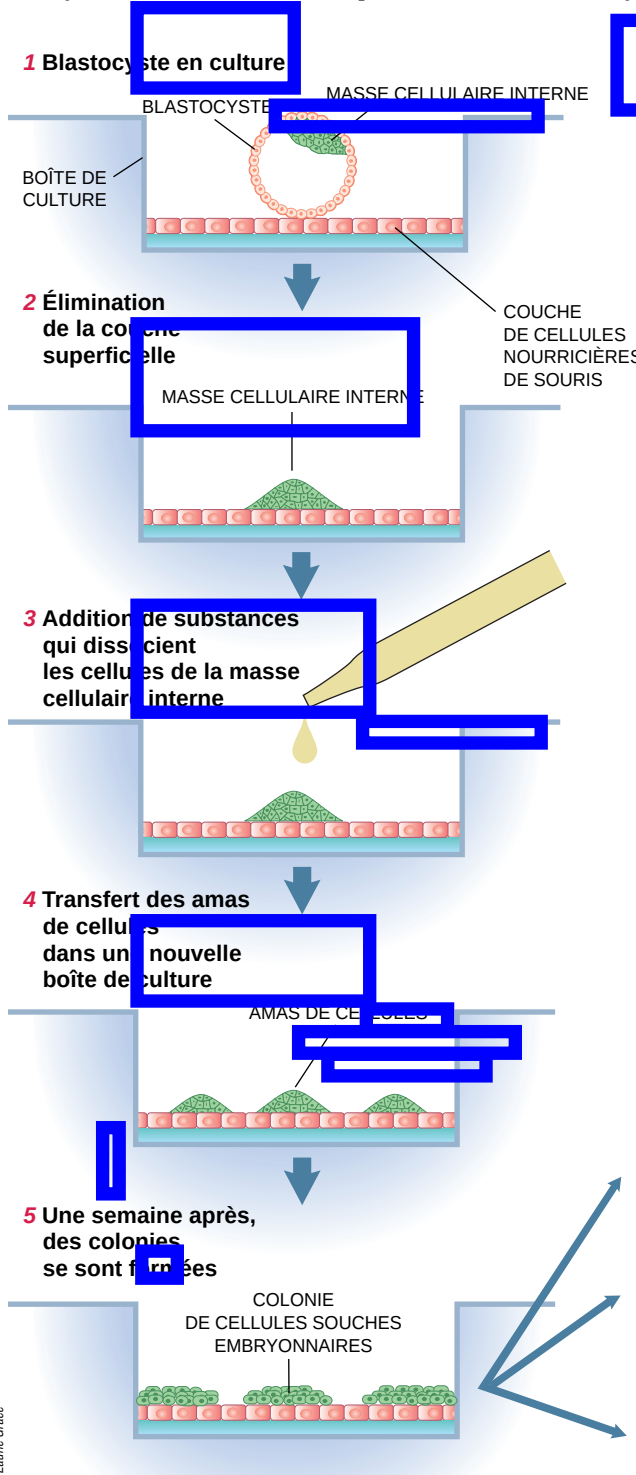
souches sont présentes dans la plupart des tissus de l'embryon. On dit que les cellules souches embryonnaires sont pluripotentes, ce qui signifie qu'elles ont de nombreuses potentialités. On attribue parfois – à tort – aux cellules souches embryonnaires de source humaine un caractère de totipotentes, ce qui sous-entend qu'elles peuvent former tous les tissus, mais elles ne jouent pas à l'origine du placenta. Ainsi, les cellules souches embryonnaires ont de nombreux points

communs avec les cellules de la masse cellulaire interne, à l'origine de toutes les cellules de l'organisme, mais elles subissent de nombreuses modifications limitant un peu leur potentialité.

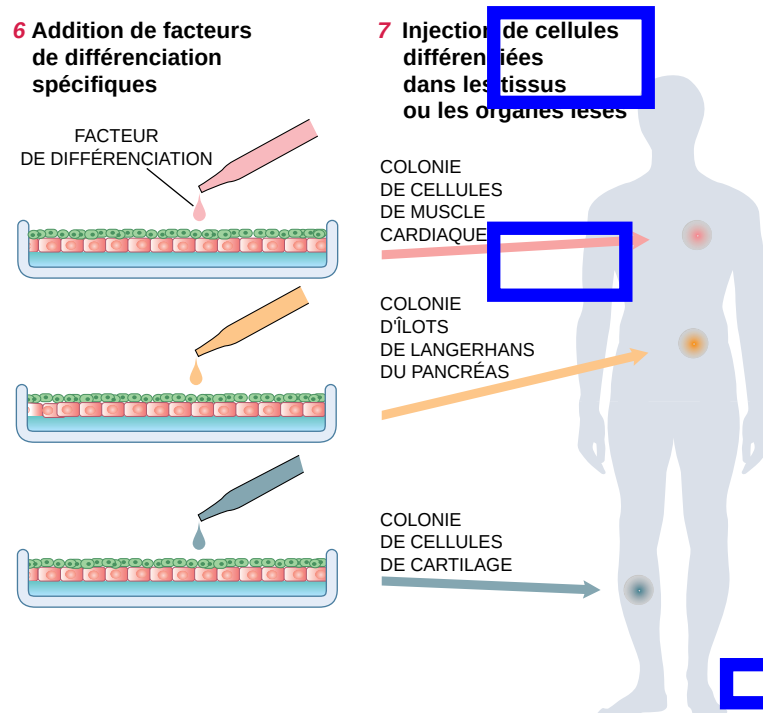
En conditions de culture, les biologistes ont trouvé qu'en l'absence d'un composé essentiel, le facteur inhibiteur de la leucémie, le LIF, les cellules commencent à se différencier de façon imprévisible. De surcroît, l'éventail des types cellulaires qui se

forment alors est beaucoup plus restreint que dans l'embryon. Les cellules sont injectées dans un blastocyste, qui est placé dans un milieu de culture est dépourvu de certaines substances biologiques indispensables et présentes seulement dans l'embryon. On s'est alors demandé comment reproduire artificiellement les conditions présentes dans un embryon.

Les progrès ont été rapides. Gerard Bain, David Gottlieb et leurs collègues



2. POUR OBTENIR DES CELLULES SOUCHES embryonnaires humaines (ci-contre, étapes 1 à 4), on laisse se développer un tout jeune embryon, nommé blastocyste. On a ouvert celui qui a été photographié (ci-dessus), afin d'observer la masse cellulaire interne. Des cellules souches embryonnaires seront peut-être un jour administrées à des personnes malades (ci-dessous, étapes 6 et 7).



de l'Université de médecine de Washington. Les cellules souches embryonnaires de souris se différencient en neurones quand on les traite par de l'acide rétinoïque (un dérivé de la vitamine A). Cette substance naturelle semble activer un ensemble de gènes spécifiques des neurones et inhiber les gènes qui s'expriment dans des cellules qui se différencient en d'autres types.

De même, certains facteurs de croissance stimulent les cellules issues de cellules souches embryonnaires et leur font engendrer divers types de cellules du sang. Les cellules souches embryonnaires pourraient même engendrer des cellules cardiaques, notamment particulièrement. Quand je regarde au microscope des cultures de cellules souches embryonnaires, je suis toujours stupéfait de voir des amas se différencier spontanément, à un rythme rapide et régulier. Les biologistes pourraient laisser ces cellules se développer, puis sélectionner les types cellulaires voulus et les laisser se multiplier.

C'est précisément ce qu'ont fait Loren Field et ses collègues de la Faculté de médecine de l'Indiana, qui ont obtenu une culture cellulaire où plus de 99 pour cent des cellules se différenciaient spontanément en cellules cardiaques.

Dans les cellules souches embryonnaires de souris qu'ils étudiaient, ils avaient introduit un gène de résistance à un antibiotique, conçu pour ne s'exprimer qu'environ dans les cellules cardiaques. Après avoir laissé les cellules se différencier et éliminé les autres par une dose notable d'antibiotique (toutes les cellules qui ne portaient pas le gène de résistance à l'antibiotique ont été détruites), l'équipe de L. Field a recueilli des cellules cardiaques quasi pures. Transplantées dans des cœurs de souris adultes, les cellules cardiaques greffées sont restées viables pendant sept semaines.

De même, au cours d'une autre expérience, des cellules souches embryonnaires transplantées dans le cerveau de souris se différencient en neurones. Beaucoup des cellules greffées prenaient une forme de neurone, et certaines produisaient une enzyme nécessaire à la synthèse de la dopamine (le neurotransmetteur produit en grande quantité dans les neurones dopaminergiques). D'autres cellules transplantées ont synthétisé une substance spécifique d'une autre classe

de neurones. De plus, les cellules greffées ont des prolongements qui ressemblent à ceux des neurones, et des ramifications des neurones qui transmettent les signaux électriques jusque dans les tissus environnants. Les cellules greffées ont un aspect de neurone, mais on n'a pas encore vérifié qu'elles fonctionnent comme des neurones. On ignore aussi quel est le facteur de croissance de souris (s'il en existe un) qui stimule la différenciation des

cellules transplantées en neurones. On ne comprend pas encore, non plus, pourquoi les neurones se développent aussi quand les cellules sont greffées à proximité.

La culture de cellules souches est plus difficile avec les embryons de primates qu'avec les embryons de souris. La couche cellulaire externe d'un blastocyste de primate ne se rompt pas aussi facilement en culture que chez

Éthique et cellules embryonnaires

On ne pourra utiliser les cellules souches embryonnaires que si la société soutient cette recherche. Beaucoup considèrent que la manipulation d'embryons humains, même aux tout premiers stades du développement (entre la fécondation et le stade blastocyste, qui correspond à une centaine de cellules), pose des questions éthiques, car ces embryons, replacés dans un utérus, se développent en êtres humains. En 1994, un conseil américain d'experts a déclaré que la recherche sur l'embryon, y compris sur la formation et sur l'étude des cellules souches embryonnaires humaines, était justifiée d'un point de vue éthique et que des fonds devaient être alloués.

Toutefois, le Congrès américain a refusé de payer les recherches sur les embryons humains. Les travaux de J. Thomson et de J. Gearhart mentionnés dans l'article, ainsi que nos propres travaux, ont été financés par le Royaume-Uni, ont décidé que la recherche sur les embryons humains méritait d'être soutenue financièrement par le gouvernement, à défaut, comme la France et l'Allemagne, d'être financée par des fonds privés.

Comme la plupart de mes confrères, je considère que la recherche sur les embryons humains est une activité scientifique légitime, en raison de son immense potentiel médical, à condition, naturellement, d'obtenir le consentement éclairé des donneurs du matériel humain utilisé à des fins de recherche. Aujourd'hui, on fabrique couramment des embryons *in vitro* pour traiter la stérilité ; ceux qui ne sont pas implantés *in utero* sont détruits, ou destinés à la recherche.

En revanche, le transfert d'embryons expérimentaux dans un utérus obéit à des règles éthiques très différentes, car la réimplantation active les mécanismes de développement. Toute manipulation sur un embryon destiné à se développer doit être inoffensive et réalisée au bénéfice de l'être humain qui en résultera.

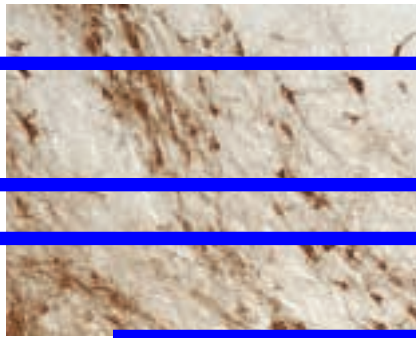
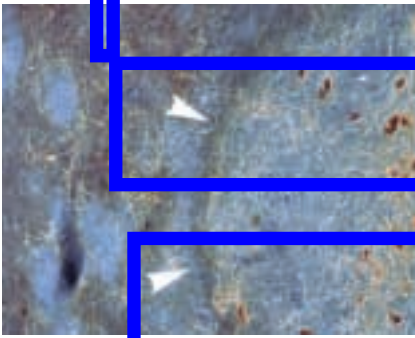
À l'évidence, le clonage des êtres humains ne satisfait pas ces exigences et, à mon avis, n'y parviendra jamais. C'est pourquoi j'ai proposé un moratoire sur le clonage des humains à des fins de reproduction : il a été approuvé par la majorité des scientifiques américains concernés.

À l' début de l'année, l'Institut de la santé américain, le NIH, a annoncé qu'il soutiendrait les travaux de recherche sur les lignes de cellules souches embryonnaires. En effet, les cellules souches embryonnaires ne sont pas équivalentes à un embryon : pour que ces cellules se développent dans un tube à essais, on doit enlever la couche cellulaire externe des blastocystes utilisés comme sources de cellules. Or les cellules retirées sont indispensables au développement du placenta, qui nourrit l'embryon, puis le fœtus, et le protège de tout rejet par le système immunitaire de la mère. Une fois les cellules externes éliminées, les cellules internes restantes ne pourraient pas se développer dans un utérus. Les cellules souches embryonnaires représentent une source de cellules différenciées et de tissus extrêmement utiles sur le plan médical, et ne soulèvent pas les questions que poserait l'utilisation d'un embryon intact.



Embryon humain, cinq jours après la fécondation.

Jason Burns, Phototake



3. DES CELLULES qui ressemblent à des neurones (en marron et en doré, à gauche) apparaissent quand des cellules souches embryonnaires de souris sont placées dans un cerveau de souris (arrière-plan bleuté). Ces cellules ont de nombreuses caractéristiques des neurones : elles ont des prolongements vers le tissu environnant (flèche) qui ressemblent à des axones, et elles produisent une enzyme (en marron, à droite) que synthétisent certains neurones.

La recherche sur les embryons humains

Aujourd'hui, en France, les lois de bioéthique interdisent les recherches sur les embryons humains précoces. Ces lois doivent être révisées prochainement et des réflexions sont d'ores et déjà organisées par le ministère de l'Éducation et de la Recherche et par l'INSERM afin d'évaluer si cette interdiction doit être levée. De ces discussions préliminaires, il ressort que l'utilisation d'embryons humains très précoces ou de cellules souches embryonnaires humaines serait justifiée pour diverses raisons, notamment pour l'amélioration des procédures d'assistance médicale à la procréation : on étudierait comment améliorer les conditions de culture des embryons et l'évaluation de la qualité des embryons à implanter ; on pourrait suivre plus méthodiquement les résultats de la fécondation avec des gamètes immatures (des précurseurs des spermatozoïdes). N'oublions pas que les résultats obtenus sur l'animal ne sont pas toujours extrapolables à l'homme.

Sur un plan plus fondamental, on pourrait étudier les mécanismes moléculaires mis en jeu aux premiers stades du développement humain, découvrir comment se développent certaines maladies génétiques ou anomalies chromosomiques. On cherchera à tout comment déclencher «à volonté» la différenciation de cellules souches embryonnaires en lignées de cellules de peau, de muscle, de cartilage, de neurones ou encore de cellules sanguines, utilisables en thérapie cellulaire et génique.

Les embryons pouvant être l'objet de recherches seraient des embryons surnuméraires pour lesquels il n'existe plus de projet parental : lors d'une tentative de fécondation, on prélève des ovules, on les préleve et féconde, mais seuls un, voire deux embryons sont planifiés, les autres sont congelés. Quand les «parents» ne veulent plus d'autres enfants, les embryons sont détruits au bout de cinq ans. Si les futures lois de bioéthique vont dans le sens souhaité par les chercheurs, ces embryons pourraient être utilisés.

D'autres embryons pourraient être issus de recherches sur les gamètes ou encore de cellules souches qui divergent être produits à des fins de recherche selon les partisans de cette possibilité. La qualité des embryons ainsi obtenus serait meilleure que celle des embryons surnuméraires issus de la fécondation *in vitro*, puisque ceux qui restent disponibles ont été écartés lors de la sélection des embryons destinés à être réimplantés.

Biologistes, médecins, juristes, spécialistes de la bioéthique s'accordent à penser que de telles recherches pourraient être justifiées. Une commission nationale de médecine et de biologie de la reproduction et de diagnostic prénatal, à condition que les parents aient donné leur accord, et que les embryons manipulés ne soient en aucune façon réimplantés chez une femme. Il nous reste quelques mois à attendre la décision des sages.

Bruno PÉAULT, INSERM U 506

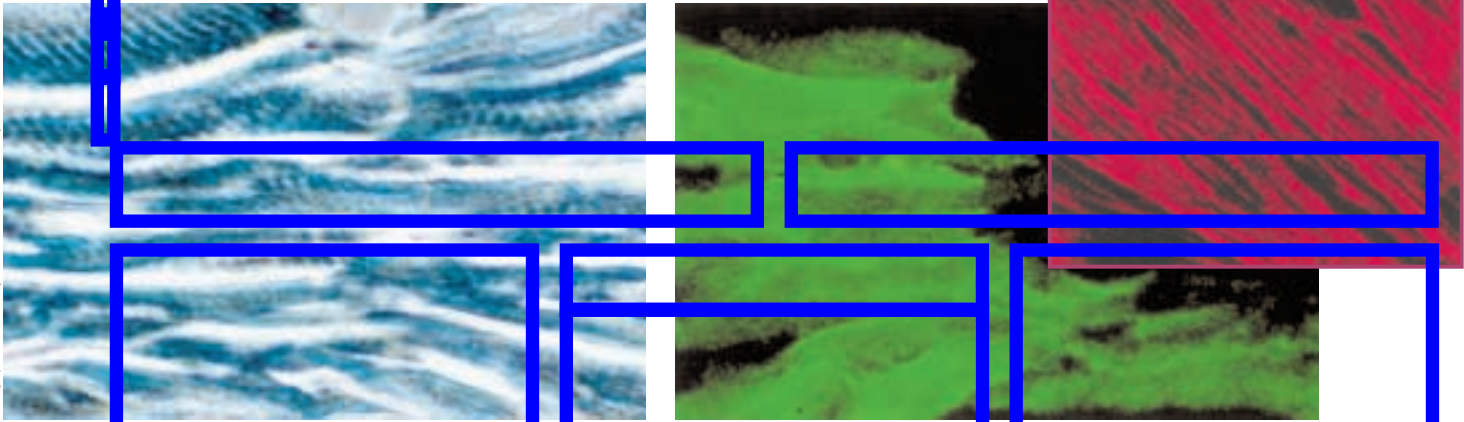
la souris, et on doit l'enlever, sinon les cellules de la masse cellulaire interne meurent. Toutefois, on espère des progrès analogues ; on saura sans doute bientôt faire produire au moins des cellules sanguines, des cellules cardiaques et des neurones. On espère aussi obtenir d'autres types cellulaires, utiles en médecine : à l'aide de cellules d'îlots de Langerhans du pancréas, on traitera le diabète ; à l'aide de fibroblastes, on soignera les brûlures et les lésions cutanées ; à l'aide de chondrocytes, on régènera le cartilage perdu au cours de l'arthrite ; à l'aide de cellules endothéliales, on réparera les vaisseaux sanguins endommagés par l'athérosclérose.

Malheureusement, les cellules souches embryonnaires ont aussi des inconvénients. Chez les souris adultes, elles forment unamas de différents types cellulaires, analogue à une tumeur, ou tératome. Avant de les utiliser à des fins thérapeutiques, on devra s'assurer qu'elles sont toutes différenciées et incapables de proliférer en un tissu incontrôlable. Une purification rigoureuse sera indispensable.

Les cellules obtenues par J. Gearhart à partir d'ovaires et de testicules en développement sont également prometteuses. Ces cellules germinales embryonnaires proviennent des précurseurs des ovules et des spermatozoïdes. J. Gearhart a montré que ce sont aussi des cellules pluripotentes : dans une boîte de Pétri, elles engendrent des cellules caractéristiques des différentes couches de l'embryon. Aujourd'hui, on ignore le devenir des cellules germinales embryonnaires injectées sous la peau d'un souris, et leur capacité à former un tissu.

Des cellules sur mesure

Toutes les cellules différenciées mentionnées seront probablement utilisées sous forme de cellules isolées à des fins thérapeutiques ; pour être efficaces, elles ne doivent pas s'organiser en un tissu de structure bien définie. Heureusement, car la formation d'un tissu est un processus complexe. En général, les organes résultent d'interactions entre des tissus embryonnaires provenant de deux couches distinctes : les poumons, par exemple, se forment lorsque des cellules issues du mésoderme interagissent avec des cellules de l'endoderme qui donneront le tube digestif. L'interaction stimule



4. LA MYOSINE, une protéine essentiellement présente dans les muscles, apparaît en rouge dans des cellules dérivées de cellules souches embryonnaires de souris (en haut, à gauche), et en vert dans

un cœur de souris, ces cellules souches s'intègrent dans le muscle cardiaque (à gauche). On les visualise par un marqueur fluorescent vert (à droite).

ces cellules endodermiques, qui se ramifient en prolongements, lesquels deviendront les poumons. Pour construire des organes, on devra apprendre à commander les interactions des cellules souches pluripotentes. La difficulté est redoutable, mais quelques embryologistes étudient le problème.

Les cellules greffées ne seront pas rejetées si le système immunitaire reconnaît qu'elles sont « compatibles ». On devrait éviter les rejets en modifiant génétiquement les cellules souches embryonnaires humaines pour qu'elles fonctionnent comme des « donneurs universels », compatibles avec n'importe quel receveur. On pourrait aussi créer des cellules souches embryonnaires génétiquement identiques aux cellules du receveur.

La création d'un type de cellules universelles nécessiterait l'inhibition ou la modification de nombreux gènes. Ces modifications empêcheraient les cellules d'exprimer à leur surface les protéines qui indiquent au système immunitaire qu'elle ne font pas partie du soi. Ces modifications seraient difficiles : on devrait sélectionner les cellules après les avoir exposées à diverses substances.

Pour fabriquer des cellules génétiquement identiques à celle du futur receveur, on pourrait aussi combiner la technique de culture des cellules souches embryonnaires avec celle de la greffe à l'aide d'une aiguille de verre mesurant un dixième du diamètre d'un cheveu, on pourrait transierer une cellule somatique (une cellule qui n'est ni un ovule ni un spermatozoïde) ou son noyau dans un œuf non fécondé dont on aurait retiré les chromosomes. L'œuf, portant seulement l'information génétique de la cellule somatique « donneuse », se

développerait après une activation par un choc électrique.

Dans plusieurs études réalisées chez l'animal, une cellule d'animal adulte a été utilisée comme donneuse de gènes, et la cellule modifiée a été implantée dans l'intérieur d'une « mère porteuse ». C'est ainsi que des biologistes ont obtenu, chez Dolly, des souris et des vaches clonées. Pour fabriquer des cellules souches destinées à être transplantées sur un receveur, il faudrait sélectionner une des cellules pour en prélever le noyau, qui serait introduit dans un œuf non fécondé, lequel commencerait à se diviser. On cultiverait l'embryon seulement jusqu'au stade blastocyste. L'embryon servirait alors à produire des cellules souches embryonnaires, génétiquement identiques aux propres cellules du receveur.

Ces cellules souches embryonnaires humaines pourraient avoir d'autres applications : comme ces cellules pourraient, théoriquement, produire un nombre illimité de cellules humaines, elles seraient utilisées pour la recherche de protéines humaines rares. De telles expériences nécessitent un grand nombre de cellules pour

que la quantité produite soit suffisante pour les analyses. Enfin, comme les cellules souches embryonnaires ressemblent aux cellules des tout jeunes embryons, elles pourraient être utilisées pour la détection de substances qui perturbent le développement et provoquent l'apparition de malformations.

Enfin, ces cellules permettraient aux biologistes d'étudier les tout premiers événements cellulaires et moléculaires du développement humain sans craindre d'enfreindre les règles de l'éthique : les expériences ne seront pas critiques, puisque les cellules souches embryonnaires ne peuvent engendrer d'embryon.

Les embryologistes examineront ainsi des questions fondamentales posées depuis des décennies : comment les cellules souches embryonnaires se différencient-elles ? Comment s'organisent-elles en organes et en tissus ?

Les enseignements tirés de l'étude des souris, des grenouilles, des poissons et des insectes sont vraisemblablement transposables en grande partie à l'homme, mais l'étude de ces mécanismes sur notre propre espèce sera bien plus satisfaisante.

Roger PEDERSEN est professeur de gynécologie et d'obstétrique à l'Université de San Francisco.

Roger A. PEDERSEN, *Studies of In Vitro Differentiation with Embryonic Stem Cells, in Reproduction, Fertility and Development*, vol. 6, n° 5, pp. 543-552, 1994.

Michael G. KLUG et al., *Genetically Selected Cardiomyocytes from Differentiating Embryonic Stem Cells Form Stable Intracardiac Grafts*, in *Journal of Clinical Investigation*, vol. 98, n° 1, pp. 216-224, juillet 1996.

T. DEACON et al., *Blastula-Stage Stem Cells Can Differentiate into Dopaminergic and Serotonergic Neurons after Transplantation*, in *Experimental Neurology*, vol. 149, pp. 28-41, janvier 1998.

M. KENNEDY et al., *A Common Precursor for Primitive Erythropoiesis and Definitive Haematopoiesis*, in *Nature*, vol. 386, pp. 488-493, 3 avril 1998.

J.A. THOMSON et al., *Embryonic Stem Cell Lines Derived from Human Blastocysts*, in *Science*, vol. 282, pp. 1145-1147, 6 novembre 1998.

Les tsunamis

FRANK GONZÁLEZ

On ne peut lutter contre des vagues hautes comme des immeubles de dix étages et rapides comme un cyclomoteur. En revanche, on évite des dégâts si l'on sait prévoir leur arrivée sur les côtes.



1. LES TSUNAMIS LES PLUS VIOLENTS détruisent tout sur leur passage (cette image est un montage photographique). Face à des vagues de 30 mètres de haut, qui se déplacent à près de 15 mètres par seconde, les populations doivent fuir aussi rapidement que possible.

Une vague plus haute que prévu Papouasie-Nouvelle-Guinée

17 juillet 1998

Hauteur maximale des vagues : 15 mètres

Nombre de victimes : 2 200



Le village de Sissano, quatre jours après le tsunami. Les taches vides étaient occupées par des constructions.

Cette bande de sable aujourd'hui dénudée, le long de la côte Nord de la Papouasie-Nouvelle-Guinée, était couverte d'habitations avant d'être balayée par trois vagues gigantesques. Le séisme d'origine de la catastrophe était de magnitude 7,1, faible par rapport à ceux qui déclenchent habituellement ce type de catastrophe. Les vibrations sismiques ont-elles déclenché d'autres phénomènes sous-marins, tels un glissement de terrain ou l'explosion d'un poche de gaz ?

D'autres tsunamis d'amplitude inattendue ont causé des désastres, comme au Nicaragua, en 1992, mais le fond marin n'a jamais été étudié précisément. Deux expéditions ont exploré le fond de la mer près du lieu de la catastrophe en Papouasie-Nouvelle-Guinée : elles ont repéré une légère dépression qui correspondrait à un glissement de terrain, sans déterminer si cette anomalie est liée à la dernière catastrophe ou si elle a été créée lors d'un séisme antérieur.

Cette soirée du 17 juillet 1998 s'annonçait tranquille pour les habitants de Sissano, d'Arop, de Warapu et des autres villages installés entre le lagon de Sissano et la mer de Bismarck, sur la côte Nord de Papouasie-Nouvelle-Guinée. Lentement, le soleil se coucha sur l'horizon... puis, brusquement, la gigantesque énergie accumulée depuis des années dans les roches sous-jacentes par la convergence des plaques tectoniques fut libérée. Le séisme principal, de magnitude 7,1, fut ressenti sur la côte du lagon à 18 heures 49. Les déformations du fond de la mer engendrèrent un gigantesque raz-de-marée.

John Sinawe, un habitant d'Arop, à l'extrémité Sud du banc de sable, a survécu à la catastrophe et a raconté ce qui s'était passé : juste après la secousse principale, la mer s'est dressée au-dessus de l'horizon, jusqu'à 30 mètres de haut, avec un bruit d'orage éloigné. Le bruit s'était ensuite transformé en un vrombissement d'hélicoptère, puis il s'était progressivement atténué, pendant que la mer se retirait en-deçà de son niveau de plus basse marée. Après quatre à cinq minutes de silence, une première vague de 15 mètres de hauteur était arrivée, accompagnée d'un grondement semblable à celui d'un avion à réaction volant en rase-mottes. Sinawe avait couru vers sa maison, mais la vague l'avait rattrapé. Une deuxième vague l'avait entraîné dans une mangrove, à un kilomètre de là, sur la plage intérieure du lagon, et avait rasé le village.

D'autres villageois furent moins chanceux. Plusieurs s'emparèrent sur les branches brisées des mangroves ; d'autres furent écrasés par les débris. Parmi les survivants, une trentaine au moins eurent atteints de gangrène et furent amputés. Des crocodiles et des chiens errants dévorèrent des cadavres avant l'arrivée des secours, ce qui compliqua le décompte des victimes, mais il est maintenant établi que le raz-de-marée a tué plus de 2 200 personnes, dont plus de 230 enfants. Les vagues de 15 mètres qui ont frappé la côte pendant 15 minutes ont surpris de nombreux habitants, et même ceux qui connaissaient le risque n'avaient nulle part où se réfugier sur le banc de sable.

Ces vagues étaient la manifestation d'un tsunami, un violent raz-de-marée. La plupart des tsunamis se produisent dans l'océan Pacifique, et 86 pour

cent d'entre eux résultent de tremblements de terre sous-marins le long de la ceinture de feu du Pacifique, où la collision de plaques tectoniques crée une zone de forte sismicité.

Depuis 1990, dix tsunamis ont tué plus de 4 000 personnes, chiffre élevé dû à l'accroissement des populations côtières. Pour la même période, 82 tsunamis ont été ressentis sur toute la surface du globe (on n'en comptait naguère que 57 par décennie, parce que les moyens de communication mondiales étaient moins bons). Depuis le tsunami qui a frappé le Nicaragua en 1992 (voir l'encadré de la page 68), un «bulletin des tsunamis» a été créé : diffusé par courrier électronique, il transmet rapidement toutes les informations disponibles aux spécialistes du monde entier, qui peuvent alors laborer ainsi plus facilement.

Les États-Unis ne sont pas à l'abri : des désastres comparables à ceux du Nicaragua ou de Papouasie-Nouvelle-Guinée ont aussi durement frappé l'île d'Hawaï et l'Alaska. En outre, les résultats récents indiquent que de telles catastrophes pourraient aussi toucher la côte Ouest des États-Unis, où le nombre

de géologues pensaient que le risque était faible. Les séismes se produiraient tous les 300 à 700 ans le long de la zone de subduction cascadienne, région de la côte Nord-Ouest du Pacifique où la plaque de l'océan Pacifique plonge sous le continent Nord-Américain. Se déplaçant à une vitesse de 5 à 10 centimètres par an, elle a été confirmée en avril 1992, lors d'un tremblement de terre de magnitude 5,4, à la pointe méridionale de la zone de subduction, provoqua un petit raz-de-marée près du cap Mendocino, en Californie. Cet événement a accéléré la mise en place du premier réseau de surveillance des tsunamis.

La vague de port

Qu'est-ce exactement qu'un tsunami? En japonais, «tsu-nami» signifie littéralement «vague de port», mais il s'agit d'une

vague, de quelques mètres de haut tout au plus, mais dont la longueur peut atteindre 750 kilomètres en plein océan, et qui se propage à travers l'océan à la vitesse d'un avion. Elle se transforme en une déferlante destructrice dans les eaux côtières. Malgré sa vitesse de déplacement, un tsunami est complètement inoffensif en eau profonde.

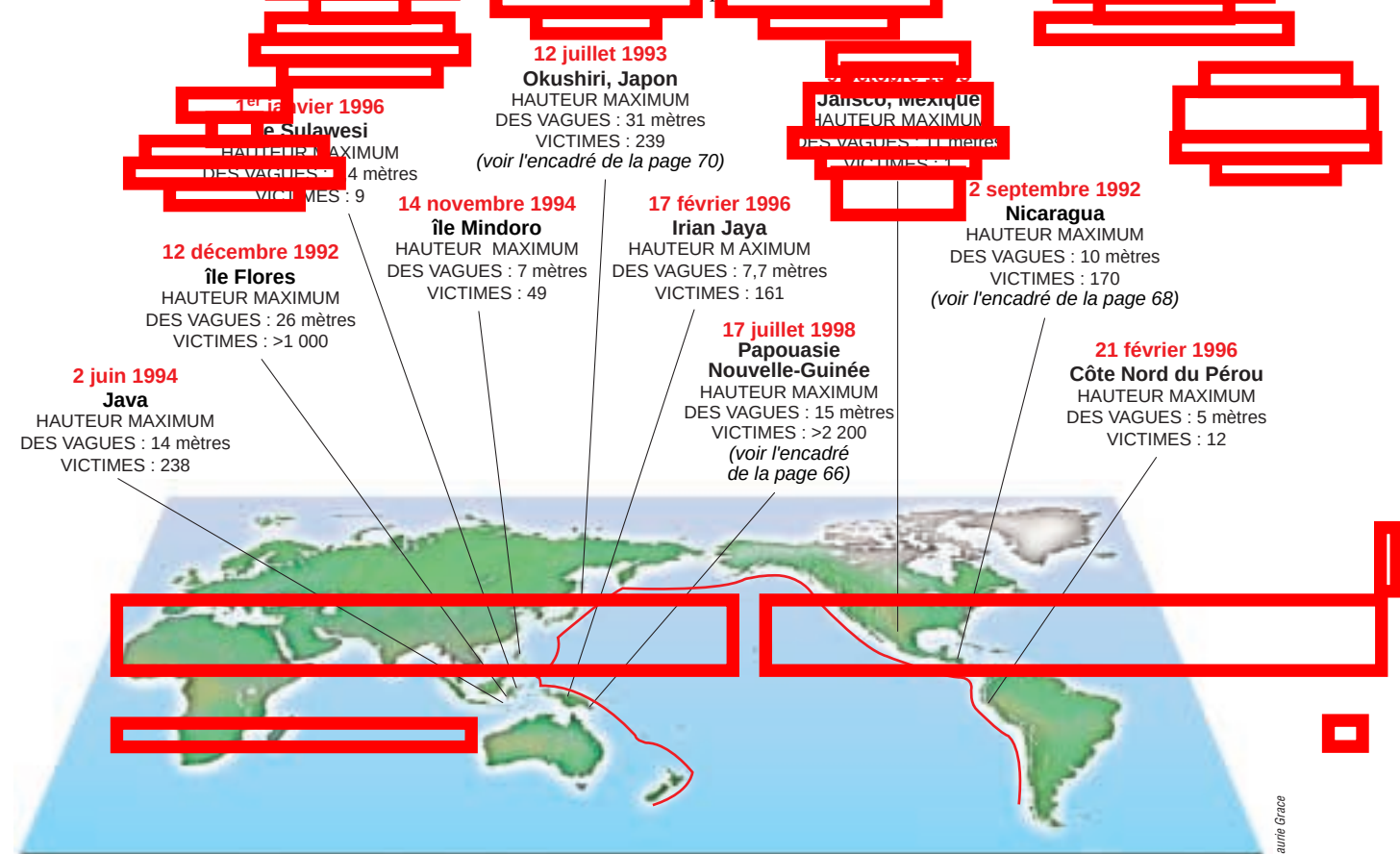
la vague, de très faible pente, passe la plupart du temps inaperçue.

Les tsunamis se propagent sur de longues distances, jusqu'à plusieurs milliers de kilomètres. L'île d'Hawaï, au milieu de l'océan Pacifique, est ainsi particulièrement exposée aux grands tsunamis qui traversent le Pacifique : elle a été touchée 12 fois depuis 1895.

Le tsunami le plus destructeur avait son origine à 700 kilomètres de là, dans la zone des îles Aléoutiennes, près de la côte de l'Alaska (voir l'encadré de la page 72). Toutefois, les tsunamis les plus dévastateurs sont ceux qui prennent naissance près des côtes, tels celui qui a frappé la Papouasie-Nouvelle-Guinée en 1998 ou celui qui a suivi l'explosion du volcan Krakatoa, en Indonésie, en 1883 (les vagues, hautes

de 12 à 13 mètres, tuèrent plus de 30 000 personnes dans un rayon de 120 à 130 kilomètres). James Lander, du Centre américain d'informations géophysiques, a calculé que 90 pour cent des victimes des tsunamis sont à moins de 200 kilomètres des zones de naissance.

Un tsunami se déplace en trois étapes : le déclenchement, par le déplacement vertical brusque de la colonne



2. DIX TSUNAMIS ONT TUÉ plus de 4 000 personnes depuis 1990. La collision des plaques tectoniques le long de la ceinture de feu du Pacifique (schématisée en rouge) déclenche fréquem-

ment des vagues meurtrières (environ une par an) qui traversent l'océan et dont la plus récente a balayé la côte de Papouasie-Nouvelle-Guinée en 1998.

Un séisme lent, silencieux et meurtrier Nicaragua

2 septembre 1992

Hauteur maximale des vagues : 10 mètres

Nombre de victimes : 170



Des survivants font la queue pour obtenir du ravitaillement.



Un village côtier, le lendemain de la catastrophe.

On doit apprendre aux habitants des régions côtières à se réfugier vers les points les plus hauts du relief quand ils ressentent un séisme. Toutefois, au Nicaragua, en 1992, le tsunami qui tua 170 personnes et laissa 13 000 sans abri n'avait été annoncé que par de faibles secousses, et la population n'avait pas perçu le danger. Cinq à dix pour cent des séismes sont ainsi silencieux.

Les vibrations caractéristiques des séismes ont une courte longueur d'onde et elles s'atténuent rapidement en se propageant ; elles n'ont pas franchi la distance qui sépare le foyer sous-marin du continent. Les ondes de longueurs supérieures ont atteint la côte, mais elles accélèrent beaucoup moins le sol et elles n'ont pas été détectées par les sismographes standards, insensibles aux périodes supérieures à 20 secondes. Ce séisme a peut-être dégagé cinq fois plus d'énergie que ne le laisse croire la magnitude de 7,0. Cet événement a clairement montré que les systèmes de détection et d'alerte aux tsunamis devaient être équipés de sismographes à large bande passante.

d'eau ; la propagation, de la haute mer vers les côtes ; le déferlement sur le rivage. La description et la modélisation de ces trois étapes permettent la prévision des conséquences d'un tsunami déclenché en un point donné, ainsi que la reconnaissance des zones à risque. L'efficacité de ces prévisions est toutefois encore limitée par les défauts de la modélisation du déclenchement et du déferlement des vagues.

Comment apparaît un tsunami ? Plusieurs phénomènes créent des vagues à la surface de la mer. Le vent, d'abord, déforme la surface de l'eau en ondes assez courtes qui ne créent que des mouvements superficiels : un plongeur en apnée attend facilement les profondeurs où la houle ne se fait plus sentir, et même les fortes tempêtes de pleine mer, qui produisent des vagues de 20 à 30 mètres plus, ne déplacent pas les eaux profondes. Les marées, en revanche, qui balaient les côtes du Globe deux fois par jour, créent, comme les tsunamis, des courants qui déplacent les eaux profondes. Elles sont toutefois régulières, soumises aux attractions conjuguées de la Lune et du Soleil, et les vagues qu'elles créent sont rarement très hautes.

Les tsunamis, événements catastrophiques qui mettent la mer en mouvement sur toute son épaisseur, sont déclenchés par une déformation du fond océanique lors du mouvement relatif de deux plaques tectoniques le long d'une faille ou, plus rarement, lors d'une éruption volcanique, de l'impact d'une météorite ou d'un glissement de terrain sous-marin. L'eau suit alors le mouvement du fond. Comme on n'enregistre jamais directement cette déformation du fond, les modèles n'en donnent qu'une description simplifiée, même dans le cas d'un séisme : on suppose que les plaques tectoniques se chevauchent suivant une surface plane rectangulaire.

Toutefois, même avec une description aussi simple, le calcul de la hauteur initiale du tsunami nécessite la connaissance de dix paramètres, telles la quantité de déplacement de part et d'autre du plan de faille ou la longueur du déplacement relatif. Immédiatement après le séisme, les enregistrements des sismographes n'indiquent que l'orientation du plan de faille, la localisation du séisme, sa magnitude et sa profondeur. Tous les autres paramètres doivent être estimés : la première simulation sous-estime souvent l'ampleur des inondations d'un facteur cinq à dix.

Dans ce modèle à un seul plan de faille, la surface de rupture, calculée à partir des enregistrements sismiques, est souvent surestimée : la précision spatiale des données sismiques est insuffisante. De ce fait, le calcul prévoit que l'énergie libérée est dissipée sur une surface plus grande qu'elle n'est ; l'amplitude du mouvement vertical du fond marin et la hauteur de la vague initiale sont sous-évaluées. C'est seulement quand le tsunami a déferlé que les données sur les inondations et les enregistrements sismiques complémentaires permettent un calcul plus précis de la hauteur initiale. L'étude des répliques permet aussi d'affiner, pendant les mois qui suivent le séisme initial, permet finalement de mieux comprendre la répartition de l'énergie sismique, en particulier, de mieux délimiter la zone de rupture de la faille. Des résultats sont obtenus en général plusieurs mois de travail, mais chaque simulation réussie accroît la fiabilité des prévisions futures.

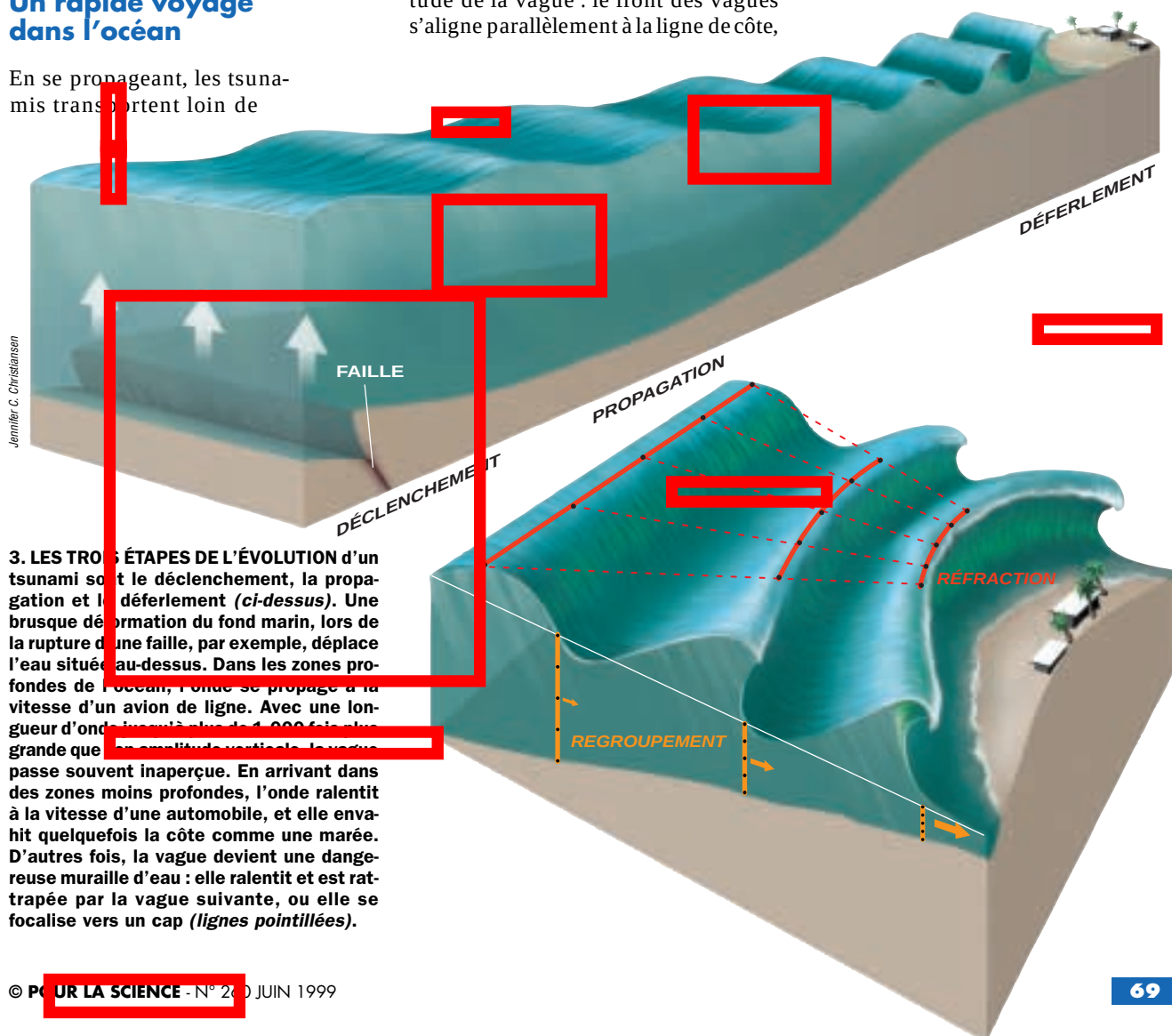
Un rapide voyage dans l'océan

En se propageant, les tsunamis transportent loin de

la source l'énergie libérée lors du séisme, comme les vibrations transportent l'énergie sismique à travers l'écorce terrestre. La hauteur de la vague est si petite par rapport à sa longueur d'onde et à la profondeur de l'eau, et la longueur d'onde est si grande par rapport à la profondeur que l'on peut utiliser la théorie des ondes longues linéaires. Celle-ci indique que la hauteur de l'onde ne détermine pas sa propagation et que sa propagation est d'autant plus rapide que la couche d'eau est épaisse et que la longueur d'onde est grande. Si l'on considère, par exemple, une onde plane, le passage de l'onde dans un plan corré d'eau nécessaire à l'élévation du niveau de la mer sur la hauteur de la vague. Or, la vitesse de propagation de l'onde dépend pas de la profondeur et, plus celle-ci est grande, plus le débit qui traverse le plan est grand, donc plus l'onde passe rapidement. Le relief sous-marin modifie la forme des vagues à l'approche des côtes, quand la couche d'eau est mince par rapport à l'amplitude de la vague : le front des vagues s'aligne parallèlement à la ligne de côte,

s'enroulant autour des caps. C'est le phénomène de réfraction. Ces déviations résultent du ralentissement des vagues qui s'arrêtent, dans les parties les plus entamées du front, engendre la rotation du front et le regroupement des vagues près de la côte : les vagues se rattrapent et se regroupent. La réfraction des ondes et le regroupement des vagues concentrent l'énergie : les vagues se dressent et des courants très intenses sont créés.

Cette dernière étape du tsunami, le déferlement, est peut-être le plus difficile à modéliser : la vague est si haute (jusqu'à plusieurs dizaines de mètres) que la théorie linéaire n'est plus applicable. Quand elle n'est pas arrêtée par des falaises côtières ou par d'autres obstacles, une vague peut pénétrer sur plusieurs centaines de mètres à l'intérieur des terres. La submersion est aussi favorisée pour les séismes de subduction : lorsque la plaque océanique avance sous la plaque continentale, le



3. LES TROIS ÉTAPES DE L'ÉVOLUTION d'un tsunami sont le déclenchement, la propagation et le déferlement (ci-dessus). Une brusque déformation du fond marin, lors de la rupture d'une faille, par exemple, déplace l'eau située au-dessus. Dans les zones profondes de l'océan, l'onde se propage à la vitesse d'un avion de ligne. Avec une longueur d'onde généralement plus de 4 000 fois plus grande que l'amplitude verticale, la vague passe souvent inaperçue. En arrivant dans des zones moins profondes, l'onde ralentit à la vitesse d'une automobile, et elle envahit quelquefois la côte comme une marée. D'autres fois, la vague devient une dangereuse muraille d'eau : elle ralentit et est rattrapée par la vague suivante, ou elle se focalise vers un cap (lignes pointillées).

fond de l'océan est soulevé au large et la côte est envahie par les vagues. L'onde forme une crête, mais vers le continent il forme une dépression. Ainsi, le retrait de la mer favorise l'arrivée d'un tsunami favorise sa pénétration dans les terres. Les modèles comme les observations semblent indiquer que la vague est d'autant plus haute et pénètre d'autant plus loin qu'elle est précédée d'un creux.

Une population avertie

La prévision des tsunamis ne sauve des vies et ne limite les dégâts matériels que si les populations sont conscientes de la menace et réagissent de façon appropriée. Ainsi, le Japon, près des zones de collision de quatre plaques tectoniques, s'est trouvé à proximité de l'océan Pacifique. Les tsunamis décrits de manière fiable

depuis 1895. Pourtant, au cours du 20^e siècle, 10 tsunamis ont frappé le Japon et ont fait de nombreux dégâts matériels ou des victimes. Ce chiffre est bien inférieur à ceux que l'on relève dans les pays qui se sont préoccupés d'informer leur population. Ainsi, près de la moitié des 34 tsunamis qui ont frappé l'Indonésie sur la même période ont fait des dégâts ou des victimes.

Cette différence résulte des moyens importants que le Japon a consacrés à la prévention.

mis : information, système d'alerte et protection des rivages, notamment par la plantation de forêts côtières et par la construction de digues. L'efficacité de ces mesures a été démontrée le 12 juillet 1993 : un séisme de magnitude 7,8, dans la mer du Japon, a fait déferler un tsunami sur la péninsule d'Okushiri (voir l'encadré ci-dessous).

Cinq minutes après la secousse principale, l'agence météorologique japonaise annonça à la radio et à la télévision qu'un tsunami était en route. Déjà, des vagues de 10 à 20 mètres avaient frappé la côte près du foyer du séisme, tuant de nombreuses personnes qui n'avaient pas eu le temps de fuir. À Aonae, petit village de pêcheurs au Sud de l'île, la plupart des habitants s'étaient réfugiés aux points les plus élevés dès qu'ils avaient ressenti les secousses. Cinq minutes plus tard, des vagues de cinq mètres de haut envahirent la zone.

centaines de commerces et d'habitations. Plus de 200 personnes périrent dans ce désastre, mais la rapidité de la réaction des habitants en sauva beaucoup plus.

Au contraire, en 1992, le tsunami qui frappa l'île de Flores, en Indonésie, tua plus de 1 000 personnes ; les survivants ont rapporté que la plupart des

L'information sauve des vies

Okushiri, Japon

12 juillet 1993

Hauteur maximale des vagues : 31 mètres

Nombre de victimes : 239

En 1993, des incendies se sont allumés après le tsunami qui a ravagé Aonae, petit village de pêcheurs sur la péninsule d'Okushiri. Des vagues de cinq à dix mètres de haut ont déferlé sur la côte moins de cinq minutes après le déclenchement d'un séisme de magnitude 7,8, entre 15 et 30 kilomètres du rivage, dans la mer du Japon. Les vagues ont submergé des digues construites après le passage d'un précédent tsunami, ont balayé les commerces, les habitations, les véhicules, les navires à quai et le matériel lourd stocké dans les docks, les transformant en autant de projectiles meurtriers et destructeurs. Les chocs provoquèrent des courts-circuits et des incendies que des débris rendirent inaccessibles aux véhicules des pompiers.

Les systèmes d'alerte et le bon comportement des habitants ont fortement limité le nombre de victimes : l'agence japonaise de météorologie avait donné l'alerte à temps, de sorte que de nombreux habitants se réfugièrent sur les hauteurs dès qu'ils ressentirent la secousse ; certains même n'attendirent pas l'alerte et s'enfuirent.

L'analyse de ce tsunami a montré que l'on peut limiter le nombre de victimes par des mesures de prévention. Les relevés détaillés des dégâts causés aux réseaux de transports et de communications, les recensements des survivants et des services de secours, les mesures du déferlement et des inondations, ainsi que des relevés aériens, ont permis de constituer une banque de données précieuse pour les autres sites à haut risque. Cette structure urbaine est en effet comparable à d'autres côtes urbanisées, contrairement aux pays moins développés touchés par des tsunamis au cours de cette décennie.



La péninsule incendiée et dévastée après le tsunami.



Un véhicule de pompiers a été endommagé par la catastrophe.

habitants de la côte n'avaient pas compris que les secousses sismiques annonçaient l'arrivée d'un tsunami et qu'ils n'avaient pas essayé de se réfugier vers l'intérieur des terres. En 1998, la population de Papouasie-Nouvelle-Guinée ignorait également les risques, de sorte que le tsunami fut considéré comme pour un événement de cette importance : lorsqu'ils ont ressenti le séisme, des villageois sont même allés observer le phénomène sur la plage ! Un séisme avait certainement, déjà, provoqué l'affaissement de la zone du lagon de Sissano en 1907, mais le tsunami résultant avait été trop faible pour faire beaucoup de victimes, et il était oublié.

Comment évaluer le danger des tsunamis ? L'analyse des événements récents est indispensable, et les consultations d'archives apportent d'autres informations précieuses. J. Landier et ses collègues ont rassemblé des informations sur plus de 200 tsunamis qui ont touché l'océan Pacifique depuis le XVIII^e siècle. Ils ont évalué à trois milliards de francs le coût cumulé des dégâts et à 470 le nombre de victimes, surtout en Alaska et à Hawaï. Dans ces régions, c'est la zone de subduction des Américaines qui menace : la probabilité qu'un séisme de magnitude au moins égale à 7,4 s'y produise avant 2008 est estimée à 84 pour cent.

Les archives ne mentionnent pas, toutefois, que la zone de subduction cascadienne menace les États de Washington, de l'Oregon et de la Californie du Nord. Brian Atwater, du Bureau géologique américain, a repéré dans l'État de Washington des dépôts de sable et de gravier qui auraient été apportés par des raz-de-marée consécutifs à des séismes de cette zone. Cette hypothèse est confortée par la découverte de dépôts analogues après les récents tsunamis de Flores, d'Indonésie, de Papouasie-Nouvelle-Guinée ou du Nicaragua. Au moins un des segments de la zone de subduction cascadienne semble être sur le point de rompre ; il risque de créer un grand séisme et un tsunami violent. Le risque est aussi élevé que dans le Sud de la Californie, où la probabilité est de 35 pour cent la probabilité que cette catastrophe survienne avant 2043.

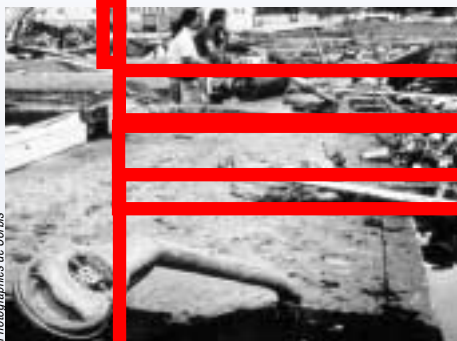
En 1992, un tsunami qui a devasté le cap Mendocino a montré aux États-Unis que des mesures s'imposaient. Les géographes de l'État de Californie ont établi des cartes qui répertorient tous les risques naturels pour les villes côtières d'Eureka et de Crescent City :

Ni le premier, ni le dernier Îles Aléoutiennes orientales

1^{er} avril 1946

Hauteur maximale des vagues : 35 mètres

Nombre de victimes : 165

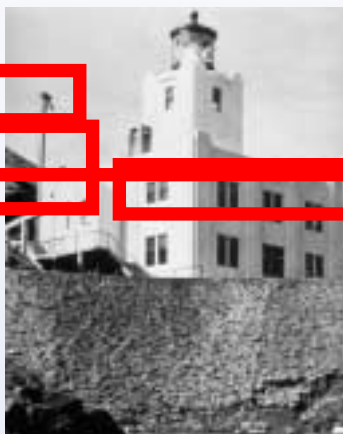


Photographies de Corbis

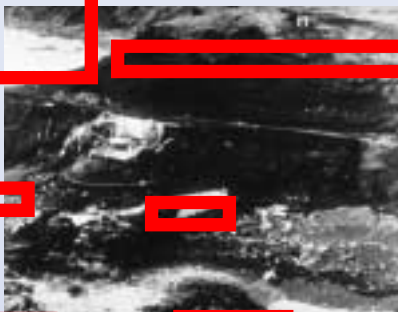
Des parcmètres ont été aplatis à Hilo, sur l'île d'Hawaii.

Plusieurs tsunamis ont frappé les rivages de la ceinture du feu du Pacifique au cours de cette décennie, mais des vagues destructrices ont laissé des traces bien en avant. Les séismes le long de la zone de subduction des Aléoutiennes ont engendré les pires tsunamis de l'histoire des États-Unis. Le 1^{er} avril 1946, un séisme de magnitude 7,8 provoqua un tsunami qui détruisit un phare en Alaska, tuant les cinq gardes-côtes qui l'occupaient. Le même tsunami arriva cinq heures plus tard à Hilo, à Hawaii, où il surprit la population. Des vagues de huit mètres de haut, chargées de débris de toutes sortes, entraînèrent des enfants qui attendaient le début de l'école et balayèrent un hôpital. En tout, 165 personnes périrent, dont 159 à Hawaii, et les dégâts s'élevèrent à 170 millions de francs.

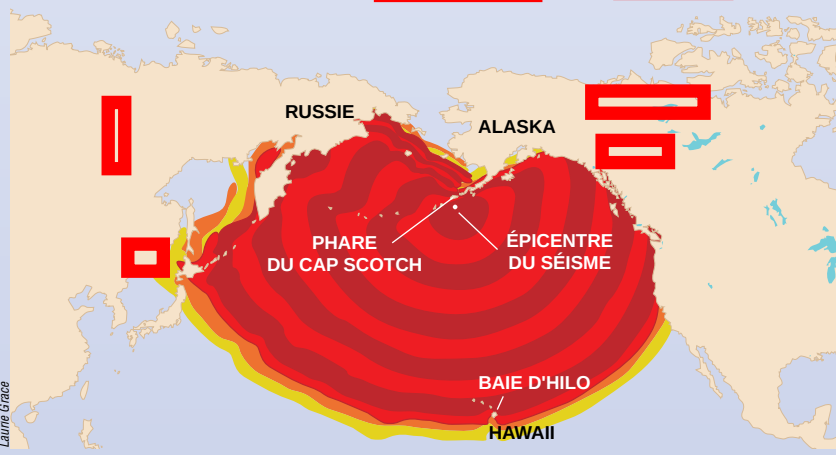
Le centre d'alerte aux tsunamis du Pacifique fut fondé en 1948, à la suite de cette catastrophe. Le centre régional d'alerte aux tsunamis d'Alaska fut fondé trois ans après la catastrophe du 28 mars 1964, qui tua plus de 100 personnes. Aujourd'hui, la reconnaissance des risques provenant de la zone sismique de la côte Ouest des États-Unis a conduit à d'autres actions préventives : cartographie des zones inondables par les tsunamis, établissement d'un réseau de détection en haute mer et campagnes de sensibilisation du public.



Le phare du cap Scotch avant le tsunami.



Le phare du cap Scotch après le tsunami.



Laurie Graze

les risques d'inondations consécutives à un tsunami, de séisme, de liquéfaction du sol ou de glissement de terrain y sont indiqués. Ces cartes indiquent les conséquences d'un fort tremblement de terre et du tsunami associé. Près de 300 000 personnes

travaillent à proximité immédiate du rivage, qui est fréquenté par environ autant de touristes. Un tsunami pourrait balayer cette population quelques minutes seulement après un grand tremblement de terre, ne laissant que très peu de temps pour donner l'alerte. Le montant des dégâts serait de 8 à 55 milliards de francs.

Un plan d'ensemble

En 1997, le Congrès des États-Unis a voté un crédit de 15 millions de francs pour la mise en œuvre d'un programme national de réduction des risques liés aux tsunamis. Ce programme, mené dans les États d'Alaska, de Californie, d'Hawaii, d'Oregon et de Washington, a trois objectifs principaux : le zonage des risques sur la côte, la détection précoce des tsunamis et la détermination de leur importance, et l'information des populations.

L'évaluation des risques se fonde sur l'élaboration de cartes de risques associées à des plans de secours et d'évacuation. De telles cartes n'ont aujourd'hui été dressées systématiquement qu'à Hawaii. Dans l'Oregon, trois villes seulement en sont pourvues. Six autres sont en cours de réalisation dans l'Oregon, en Californie et dans l'État de Washington. En Alaska, enfin, trois cartes seront dressées.

La confirmation fiable et rapide de l'arrivée d'un tsunami est indispensable aux responsables des services d'alerte. Des marégraphes ont été adaptés à la détection des tsunamis, et le réseau de détection des séismes a été renforcé : il donnera plus rapidement des informations plus complètes sur les caractéristiques des séismes. Ces équipements sont indispensables, mais les sismographes ne détectent que les tremblements de terre de forte magnitude. Les marégraphes ne détectent les tsunamis que près de la côte : ils n'apportent aucune information sur les vagues éloignées. Aussi, depuis les années 1950, 75 pour cent des alertes ont été déclenchées à tort. Cette proportion excessive décrédibilise le système d'alerte, fait courir des risques aux populations et coûte cher. La fausse alerte qui a provoqué

Les tsunamis en France

Les côtes du Pacifique subissent en moyenne un tsunami par an. Au centre de cet océan, les îles de la Polynésie française sont donc exposées au risque. Les tsunamis les plus destructeurs des 100 dernières années dans la région se sont produits notamment en avril 1946 et en mai 1960. Le tsunami d'avril 1946, déclenché au large des îles Aléoutiennes, a provoqué des dégâts importants dans tous les archipels du Pacifique, y compris dans les îles du nord des Marquises. Le 22 mai 1960, un séisme de magnitude 10 environ s'est produit au large du Chili faisant, avec le tsunami associé, plus de 2 000 victimes dans ce pays. Le tsunami, qui s'est propagé à travers l'océan Pacifique, a causé des dégâts matériels importants sur les côtes éloignées du Japon, des Philippines et d'Hawaï, et a tué plus de 200 personnes au total. Aux Marquises, le niveau des inondations dans les baies de Nuku-Hiva et de Hiva-Oa a atteint sept à dix mètres.

Plus récemment, le 20 juillet 1995, un séisme de magnitude 8,1, au large du Chili, engendra un tsunami dont les vagues atteignirent à deux ou trois mètres dans le port de la baie de Papeete, sur l'île de Tahiti.

Des bateaux furent emportés par un tourbillon formé derrière la jetée ; deux ou trois coulèrent. Dans la même baie, des vagues d'un à deux mètres furent observées le 21 février 1996 pour un séisme de magnitude 6,6 au large du Pérou.

Sur l'ensemble de la Polynésie, c'est dans l'archipel des Marquises que les amplitudes des vagues associées aux tsunamis sont les plus fortes. Les Marquises sont des îles hautes dont les côtes plongent dans l'océan avec une faible pente, de dix degrés et qui présentent de grandes baies ouvertes vers l'océan, dépourvues de barrières de récifs. Ces deux caractéristiques amplifient les tsunamis. Dans les autres archipels de la Polynésie française (les Gambier, îles de la Société, îles Australes et archipel des Tuamotu), l'énergie des tsunamis est partiellement réfléchiée par des côtes pentues (environ 30 degrés) aux profils plutôt convexes, et les conséquences en sont donc atténuées.

Une antenne du Laboratoire de détection et de géophysique du Commissariat à l'énergie atomique, installée à Tahiti, monitorise et surveille ce risque. Les ondes sismiques se propageant beaucoup plus vite que les ondes hydrauliques, la détection rapide des premières alertes de l'arrivée d'un tsunami. Sur ce principe, les données du réseau sismique polynésien sont utilisées pour la localisation du séisme en temps réel, la détermination de ses principaux paramètres (en particulier, sa magnitude) et l'évaluation du

déclenchement. Ces données sont aussi utilisées pour les forts séismes, potentiellement générateurs de tsunamis.

Parallèlement, des simulations numériques ont permis de réaliser à la simulation numérique et établit des cartes d'inondation pour les Marquises. Un tsunami équivalent à celui de 1960 causerait aujourd'hui, en Polynésie française, des dégâts importants et vraisemblablement de nombreuses victimes en mer.

En France métropolitaine, en revanche, le risque de tsunami d'origine tectonique est quasi nul. Le dernier tsunami important en Europe s'est produit en 1755. Il a été déclenché par un séisme au large de Lisbonne et il a fait plus de 5 000 victimes sur les côtes du Portugal, de l'Espagne et du Maroc. Il fut à peine observé sur les côtes françaises, assez éloignées de sa zone d'origine.

Toutefois, notre pays n'est pas à l'abri de raz-de-marée déclenchés par des glissements de terrain sous-marins, tel

celui d'octobre 1979 dans la Baie des Anges, en Méditerranée. Au large de Nice, un glissement de terrain a entraîné la destruction d'une partie du chantier du nouveau port de Nice, en face de l'aéroport : la digue en construction s'est effondrée sous la mer, causant la mort d'une

personne sur le chantier. À peu près simultanément, un mini raz-de-marée a été observé le long d'une portion de côte de 60 kilomètres, entre Cannes et Menton. À dix kilomètres du chantier, la ville d'Antibes a été inondée par une vague de deux mètres de haut environ.

Le mécanisme exact de cette catastrophe n'est pas encore

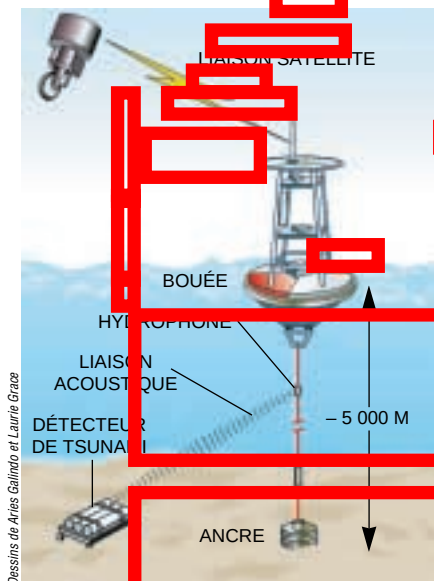
totallement déterminé. Selon nos simulations numériques, l'inondation observée vers l'aéroport s'explique par l'effondrement de dix millions de mètres cubes : trois millions de mètres cubes de remblai et sept millions de mètres cubes de sédiments sous-jacents, situés entre 0 et 150 mètres de profondeur. Toutefois, les inondations observées dans la baie ne semblent explicables que par le déplacement de 50 à 100 millions de mètres cubes de sédiments.

sur les fortes pentes au large de Nice. La forme de la baie à Antibes aurait amplifié ces oscillations et favorisé la pénétration de la mer dans la ville. L'effondrement des remblais apportés pour la construction du port de Nice a-t-il déclenché cette avalanche sous-marine plus importante ou, au contraire, les remblais ont-ils été emportés par l'effondrement des couches sous-jacentes ?

Philippe HEINRICH, Laboratoire de détection et de géophysique, CEA



Le 16 octobre 1979, une vague de deux mètres de haut à balayé les rues d'Antibes, suite à un glissement de terrain sous-marin.



Dessins de Arias Gallardo et Laurie Graze



Michelle G. Bullock, NOAA Corps

4. DES DÉTECTEURS SOUS-MARINS (à gauche) et un réseau de surveillance sismique (triangles bleus sur la carte) renforcé devraient améliorer la détection précoce des tsunamis au large des États-Unis. Les détecteurs sous-marins sont constitués de capteurs posés au fond de la mer, qui envoient par signaux acoustiques leurs enregistrements à une bouée de surface (photographie à droite) ; celle-ci transmet les informations par satellite aux services responsables du déclenchement des alertes.

l'évacuation d'Honolulu, le 7 mai 1986, a ainsi coûté plus de 200 millions de francs en salaires et en transactions commerciales perdues.

Pour améliorer la situation, les États-Unis installent aujourd'hui un réseau de six stations sous-marines de détection des tsunamis et d'alerte : le système DART (l'acronyme anglais de «détection et alerte des tsunamis en pleine mer») devrait être opérationnel et fiable d'ici deux ans. Les sismographes répartis autour de la ceinture de feu du Pacifique permettent de localiser presque instantanément un grand tremblement de terre en Alaska. En quelques instants, avant que l'on n'observe la moindre vague, des programmes informatiques calculent le temps qu'il mettrait un tsunami déclenché par le séisme pour atteindre Hawaii. Près des côtes, des marégraphes détectent l'arrivée d'un tsunami après quelques minutes, et des détecteurs placés en haute mer révèlent le passage d'ondes dangereuses.

Ces détecteurs mesurent, au fond de la mer,

ciée à la déformation de la surface de l'eau, lorsque la vague passe : cette variation de pression est transmise à un cristal piézoélectrique, dont la fréquence propre de vibration est ainsi modifiée. Même à 6 000 mètres de profondeur, ils détectent un tsunami de seulement un centimètre de haut. Les bateaux et la houle ne perturbent pas

ces mesures, car ils sont de trop petites dimensions pour que les variations de pression qui leur sont associées parviennent au fond : les longueurs d'onde des ondes associées sont courtes et seule la surface de l'eau est mise en mouvement.

Nous avons placé les premiers capteurs au fond du Pacifique Nord en 1986, et nous enregistrons le passage des tsunamis depuis cette date. Toutefois, avec ces systèmes, nous devons repêcher les appareils pour accéder aux informations. Afin de suivre en direct le passage des tsunamis, nous avons alors équipé ces capteurs d'un émetteur acoustique qui envoie les mesures à une bouée ancrée à proximité ; cette dernière transmet les informations par satellite vers des stations au sol. Les bouées relais, la liaison satellite et les capteurs sous-marins ont prouvé leur fiabilité dans de nombreux systèmes de mesure. 10 bouées météorologiques déployées le long de l'Équateur ont renseigné sur le phénomène climatique El Niño.

Deux prototypes de transmetteur acoustique que nous avons testés sont tous tombés en panne assez rapidement ; nous améliorerons aujourd'hui cette partie de l'appareillage.

D'ici à deux ans, nous installerons cinq stations dans le Pacifique Nord, de l'Ouest des Aléoutiennes à l'Oregon, et une sixième le long de l'Équateur, afin

d'intercepter le passage des tsunamis déclenchés au large de l'Amérique du Sud. Si nous pouvions disposer plus de bouées, nous réduirions le risque que des tsunamis ne nous échappent, mais nous ne pouvons pas. Nous avons donc recours à la modélisation numérique : les simulations permettront d'obtenir des prévisions plus précises pour aider les services de protection civile, qui n'ont souvent que quelques minutes pour décider de déclencher ou non une alerte, et ainsi sauver des vies.

Frank GONZÁLEZ dirige le programme de recherche sur les tsunamis et le Centre de cartographie des inondations associées aux tsunamis du Laboratoire d'environnement marin du Pacifique, à Seattle.

James F. LINDER et Patricia A. LOCKRIDGE, *United States Tsunamis (Including United States Possessions) : 1690-1988*, NOAA/National Geophysical Data Center, Publication 14-12, 1988.

F.I. GONZÁLEZ et E.N. BERNARD, *The Cape Mendocino Tsunami in Earthquakes and Volcanoes*, vol. 23, n°3, pp. 135-138, 1992.

Roy HYNDMAN, *Les tremblements de terre géants du Nord-Ouest du Pacifique*, in *Pour la Science*, février 1996.

Walter C. DUDLEY et Min LEE, *Tsunami!*, University of Hawaii Press, 1998.

Le syndrome postpolio

LAURO HALSTEAD

Plusieurs décennies après avoir retrouvé leur force musculaire, les personnes qui ont eu la poliomyélite se sentent souvent fatiguées et ressentent des douleurs. La dégénérescence des neurones moteurs semble être la cause de cet état.

Au cours de la première moitié du XX^e siècle, la poliomyélite semble être un fléau incontrôlable : la maladie frappe d'abord la région de New York, en 1916 ; puis, au fil des ans, les épidémies se multiplient et font de plus en plus de victimes. En 1952, une épidémie touche, par exemple, plus de 50 000 personnes aux États-Unis, tuant plus de dix pour cent de personnes infectées. La poliomyélite devient une hantise : on s'enferme chez soi, les piscines sont fermées, les manifestations publiques sont annulées. Les enfants sont les premières victimes.

Puis, en 1955, le vaccin par injection de virus inactivés de Jonas Salk commence à être administré ; six ans plus tard apparaît le vaccin par voie orale d'Albert Sabin, contenant du virus atténué. L'épidémie est enrayée : aux États-Unis, au milieu des années 1960, le nombre de nouveaux cas de poliomyélite est tombé à seulement un pour dix millions de personnes par an. Aujourd'hui, pour le public, la poliomyélite n'est plus une maladie, mais un vaccin. Sur le plan médical, on considère la poliomyélite comme un trouble neurologique dont l'évolution a été stoppée. On pensait qu'après la rééducation, l'état neurologique et fonctionnel de la plupart des survivants serait définitivement stabilisé.

Nos connaissances de la poliomyélite n'en restèrent là pendant quelques années, puis les choses ont brusquement évolué. Vers la fin des années 1970, les médecins recurent en consultation des personnes qui avaient eu une poliomyélite plusieurs dizaines d'années auparavant et qui commençaient à ressentir une fatigue excessive, des douleurs musculaires et articulaires et, à nouveau, une grande faiblesse musculaire. Pendant quelque temps, les médecins ne surent identifier cet ensemble inconnu de symptômes.

La multiplication des personnes souffrant des effets tardifs de la poliomyélite finit par attirer l'attention de la communauté médicale. Au début des années 1980, on regroupa sous le nom de syndrome postpolio cet ensemble de symptômes qui apparaissent généralement 30 à 40 ans après la phase aiguë de la maladie. Les malades ressentent une faiblesse musculaire progressive, une fatigue invalidante et des douleurs, surtout dans les muscles et dans les articulations. Une atrophie musculaire, des difficultés respiratoires, des troubles de la déglutition et une intolérance au froid sont des signes moins fréquents.

Les personnes ayant le risque le plus important de souffrir d'un syndrome postpolio sont celles qui ont eu les paralysies les plus graves. Les symptômes apparaissent souvent après un événement normalement sans conséquence, tels un petit accident, une chute, une période où la personne reste alitée, ou une intervention chirurgicale.

J'ai moi-même un syndrome postpolio. J'ai contracté la maladie, à 18 ans, au cours de l'épidémie de 1954, alors que je voyageais en Europe. Ma guérison exigea six mois : après avoir eu besoin d'une assistance respiratoire, je

me suis déplacé dans un fauteuil roulant, puis j'ai eu un appareillage pour marcher et, finalement, j'ai été à nouveau autonome. Mon bras droit est resté paralysé, mais le reste de mon corps a retrouvé la force et l'endurance que j'avais avant la maladie. Je me croyais guéri. Je retournai à l'université, j'apprenais à écrire de la main gauche et j'ai même appris à jouer au squash. Trois ans exactement après le début de ma maladie, je gravis le Fuji Yama, au Japon, effectuant ainsi 4 000 mètres d'ascension !

Je fis des études de médecine et oubliai ma maladie passée. Puis, il y a quelques années, j'ai commencé à ressentir une nouvelle faiblesse dans les jambes. En l'espace de quelques mois, j'en fus à nouveau réduit à utiliser un engin motorisé pour me déplacer sur mon lieu de travail.

Historique

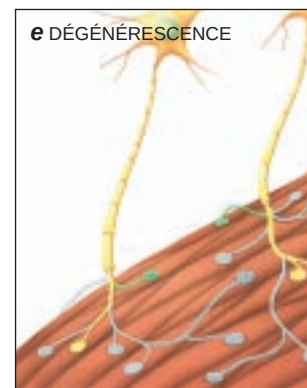
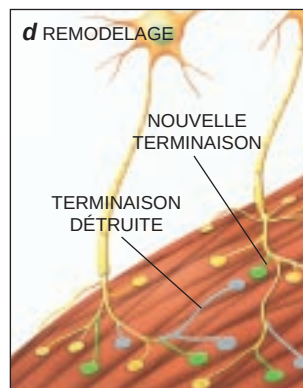
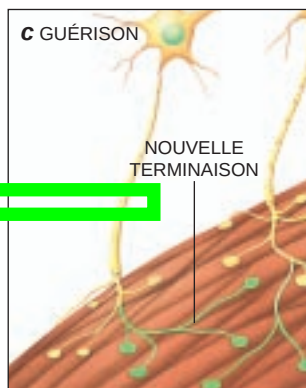
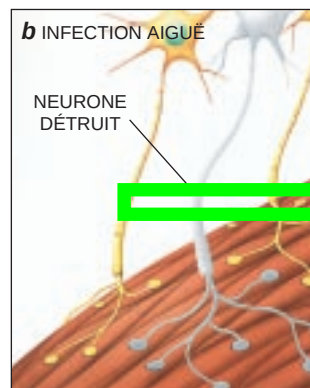
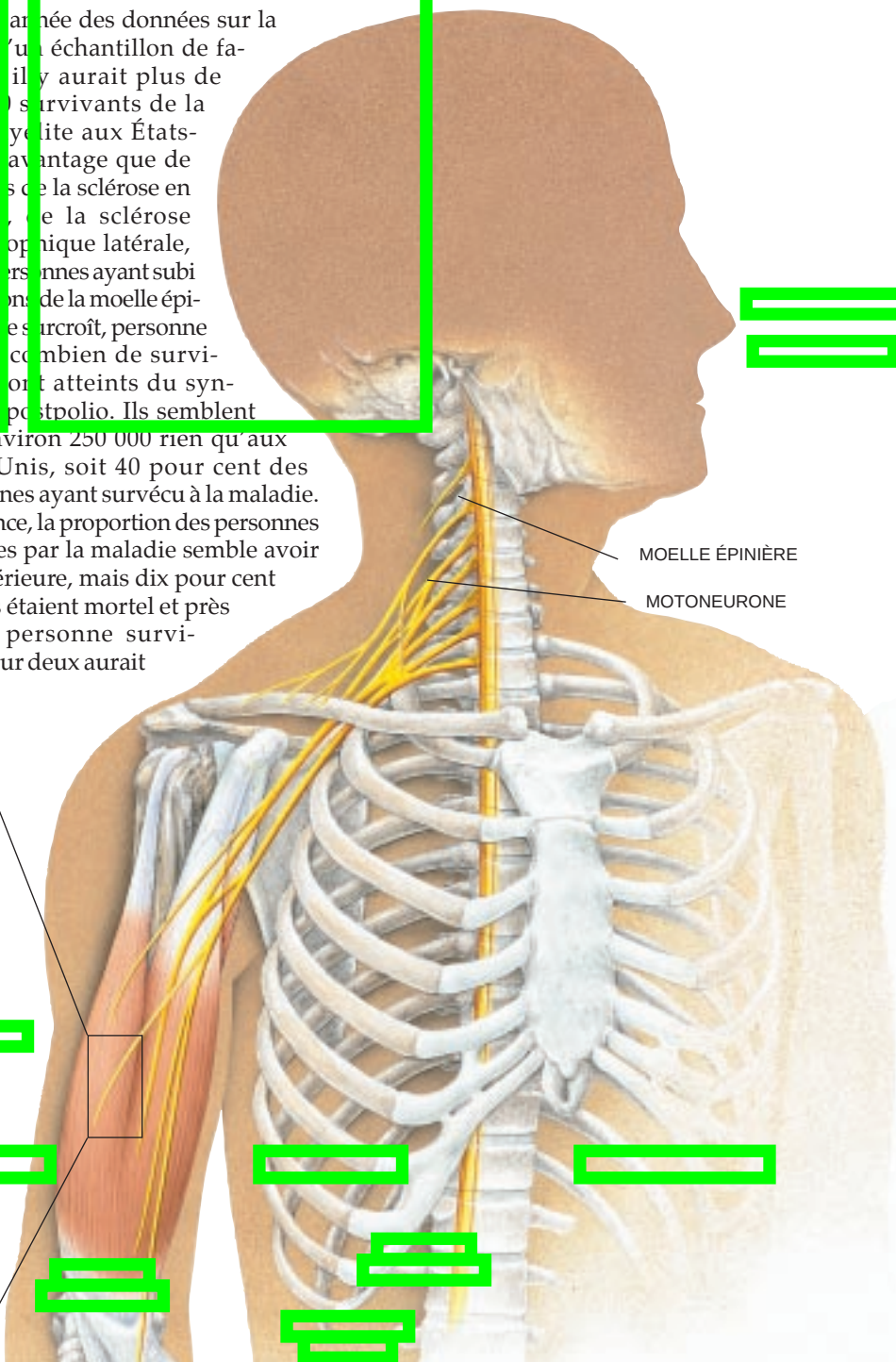
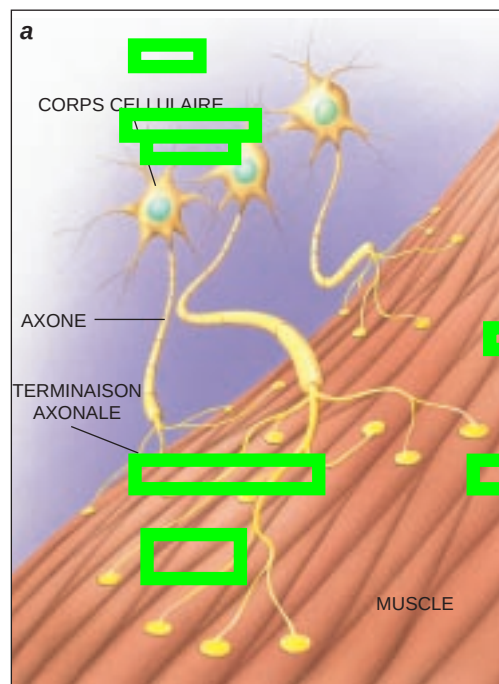
En fait, le syndrome postpolio n'est pas une nouvelle maladie. Il fut décrit par les médecins français Raymond et Charcot, en 1875, puis, comme c'est souvent le cas, il fut oublié. Pendant les 100 ans qui suivirent, environ 35 cas furent publiés. En 1984, ayant pris

1. LES MOTONEURONES (en jaune, a) qui commandent les mouvements volontaires ont leur corps cellulaire dans la moelle épinière et de longs axones qui atteignent les muscles (ici, ceux du bras). Des ramifications de l'extrémité de chaque axone activent les cellules musculaires. Certains motoneurones infectés par le virus de la poliomyélite survivent, mais d'autres meurent, entraînant la paralysie des fibres musculaires (b). De nouvelles ramifications (en vert) se développent sur les axones des motoneurones qui résistent, établissant de nouvelles connexions avec les fibres musculaires qui n'étaient plus innervées (c). Un unique motoneurone peut alors actionner cinq à dix fois plus de cellules musculaires qu'avant la maladie, créant une unité motrice géante. Ces connexions évoluent par un mécanisme de remodelage, l'unité motrice perd constamment d'anciennes connexions, tandis que de nouvelles se forment (d). Après avoir fonctionné correctement pendant plusieurs années, les unités motrices géantes commencent à dégénérer, et la faiblesse musculaire réapparaît. La lésion est soit progressive, soit fluctuante. Une lésion progressive se produit lorsque la vitesse de régénération normale des terminaisons axonales devient inférieure à celle de leur disparition ou qu'un fonctionnement incorrect n'est plus compensé (e). Une lésion fluctuante apparaît lorsque la synthèse ou la libération de l'acétylcholine, le neuro-médiateur de la contraction musculaire, devient insuffisante.

conscience des effets tardifs de la poliomyélite, nous avons organisé un congrès international à l'Institut de rééducation de Warm Springs, le centre de traitement de la poliomyélite, fondé par Franklin Roosevelt, qui avait lui-même été atteint par la maladie en 1921, à l'âge de 39 ans. Ayant retrouvé une partie de ses forces grâce à des séances de natation dans les eaux chaudes de Warm Springs, en 1926, Roosevelt acheta un hôtel dans les environs et y créa une fondation pour l'étude et le traitement de la poliomyélite. Une deuxième conférence internationale s'est tenue dans le même institut en 1986, et, au cours des années suivantes, la recherche fondamentale et clinique sur les effets tardifs de la poliomyélite s'intensifie.

On ignore le nombre exact de personnes encore vivantes qui ont eu la poliomyélite. Selon l'Institut américain des statistiques de santé, qui collecte

chaque année des données sur la santé d'un échantillon de familles, il y aurait plus de 640 000 survivants de la poliomyélite aux États-Unis, et davantage que de victimes de la sclérose en plaques, de la sclérose amyotrophique latérale, ou de personnes ayant subi des lésions de la moelle épinière. Le surcroît, personne ne sait combien de survivants sont atteints du syndrome post-polio. Ils semblent être environ 250 000 rien qu'aux États-Unis, soit 40 pour cent des personnes ayant survécu à la maladie. En France, la proportion des personnes atteintes par la maladie semble avoir été inférieure, mais dix pour cent des cas étaient mortel et près d'une personne survivante sur deux aurait



aujourd'hui un syndrome post-polio (voir l'encadré de la page 80).

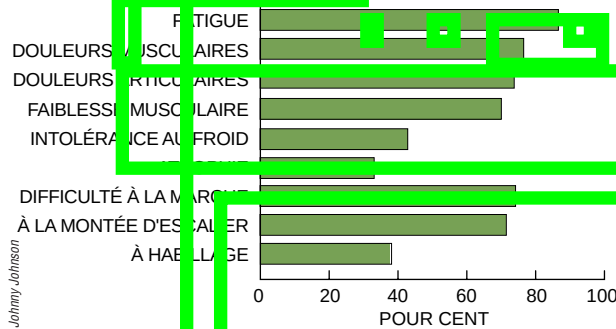
Les mécanismes d'action du virus de la poliomyélite aident à comprendre les causes possibles du syndrome postpolio. Ce petit virus à ARN pénètre dans l'organisme lors de l'ingestion d'eau et de nourriture contaminées, ou même par contact de mains souillées avec la bouche. Chez la plupart des personnes infectées, le virus ne provoque aucun symptôme, ou de la fièvre pendant quelques jours et des troubles gastro-intestinaux qui disparaissent spontanément : le poliovirus, qui se réplique dans la gorge et dans l'intestin grêle, est évacué par les selles, mais il peut atteindre le sang et diffuser dans tout l'organisme. Chez un à deux pour cent des personnes infectées, le virus envahit le système nerveux central et déclenche des paralysies.

Les mécanismes de l'infection

En cas d'infection aiguë, le virus s'attaque aux cellules nerveuses qui commandent les muscles, ou motoneurones. Ces cellules ont leur corps cellulaire dans la corne antérieure de la moelle épinière, et un long prolongement, ou axone, qui s'étend jusqu'aux muscles. Près de l'extrémité de chaque axone, de fines ramifications assurent les connexions avec les cellules musculaires. À l'interface du nerf et du muscle, nommée synapse, les prolongements de l'axone libèrent de l'acétylcholine, un neurotransmetteur qui provoque la contraction des fibres musculaires. Un motoneurone et l'ensemble des cellules musculaires qu'il active forment une unité motrice.

Avec une précision étonnante, le poliovirus envahit les motoneurones, laissant intacts les neurones adjacents qui commandent les fonctions sensitives, intestinales, urinaire et sexuelle. On s'est longtemps interrogé sur l'origine de cette spécificité jusqu'à ce que l'on découvre, récemment, les récepteurs du poliovirus sur la synapse neuromusculaire. Ces récepteurs semblent permettre au virus de pénétrer dans l'axone et de migrer jusqu'au corps cellulaire du neurone, dans la corne ventrale de la moelle épinière. Le poliovirus infecte plus de 95 pour

PROPORTION DES SYMPTÔMES DU SYNDROME POSTPOLIO



2. LES SYMPTÔMES les plus fréquents du syndrome postpolio sont la fatigue, des douleurs musculaires, des douleurs articulaires, une grande faiblesse. Les malades ont des difficultés croissantes à marcher et à monter les escaliers.

cent des motoneurones de la moelle épinière et de nombreux neurones, dans le cerveau. Soit les cellules infectées se débarrassent du virus, soit elles meurent.

L'étiologie de la paralysie est imprévisible. Sous l'action d'un stimulus inconnu, de nouveaux prolongements apparaissent sur les axones des motoneurones qui survivent. Ces nouvelles connexions rétablissent le contact avec les fibres musculaires qui ont perdu tout contact avec leurs motoneurones originels. L'établissement de ces nouveaux contacts révèle que l'organisme est programmé pour assurer la survie et le fonctionnement du nombre maximal de fibres musculaires «orphelines». Des motoneurones qui activaient initialement 1 000 cellules musculaires peuvent être connectés à 5 000, voire à 10 000 cellules musculaires. Ces énormes unités motrices permettent parfois à un nombre limité de motoneurones d'être aussi efficaces que tous les motoneurones présents avant la maladie.

Le développement des cellules musculaires sous l'action d'un exercice physique régulier favorise également le rétablissement de la motricité. Ces deux mécanismes d'adaptation – l'augmentation de taille des cellules musculaires et du nombre des ramifications axonales – sont si efficaces qu'un malade peut perdre jusqu'à 50 pour cent de ses motoneurones initiaux sans que les muscles présentent des signes cliniques d'affaiblissement. Toutefois, ces adaptations évoluent : après la phase aiguë de la poliomyélite et après la récupération initiale, un mécanisme permanent de remodelage des unités motrices se met en place ; certaines connexions sont perdues, tandis que de nouvelles apparaissent. C'est ce mécanisme de

remodelage, ou régénération permanente, qui permet aux unités motrices de produire une force musculaire constante. Lorsque cet équilibre est perturbé, la faiblesse musculaire réapparaît.

Le syndrome postpolio semble correspondre à une lente dégénérescence des connexions entre les axones et les cellules musculaires. À l'Université de l'Ohio, David Waeche et Susan Hubbell avaient proposé cette explication au début des années 1980, après avoir constaté que le fonctionnement des motoneurones des restes de la poliomyélite se détériore progressivement. Plus récemment, à l'Hôpital neurologique de Montréal, Daria Trojan et Neil Cashman ont analysé des biopsies musculaires et des enregistrements électromyographiques, et postulé l'existence de deux types de dégénérescence des motoneurones : une lésion progressive et une lésion fluctuante.

D'une part, la lésion progressive survient droit lorsque la régénération normale des connexions entre l'axone et les cellules musculaires est perturbée et que les connexions qui fonctionnent mal ne sont pas remplacées. Cette interruption des mécanismes de réparation se manifesterait par une faiblesse musculaire progressive et irréversible. D'autre part, la lésion fluctuante serait due à une synthèse ou à une libération insuffisante d'acétylcholine : la faiblesse et la fatigue musculaires sont soulagées, dans certains cas, par l'administration de médicaments, telle la pyridostigmine, qui augmentent l'efficacité de l'acétylcholine lors du déclenchement des contractions musculaires. Quelques équipes testent l'efficacité d'une autre classe de substances, les facteurs de croissance du nerf, qui stimulent à la fois la croissance des cellules nerveuses et les cellules musculaires.

Pourquoi les connexions axonales dégénèrent-elles ? Peut-être parce que les motoneurones restants seraient stimulés excessivement. Après la guérison, les motoneurones qui restent fonctionneraient davantage que des neurones normaux pour assurer les activités quotidiennes. Après plusieurs années d'utilisation excessive, ces motoneurones subiraient une sorte d'épuisement métabolique et deviendraient

incapables de remplacer les connexions qui dégèrent. On ne sait pas mesurer directement la fatigue métabolique des motoneurones, mais cette théorie est corroborée par l'observation d'anomalies sur des biopsies musculaires, par des enregistrements électromyographiques et par des examens cliniques pratiqués pendant un exercice physique.

L'épuisement des motoneurones

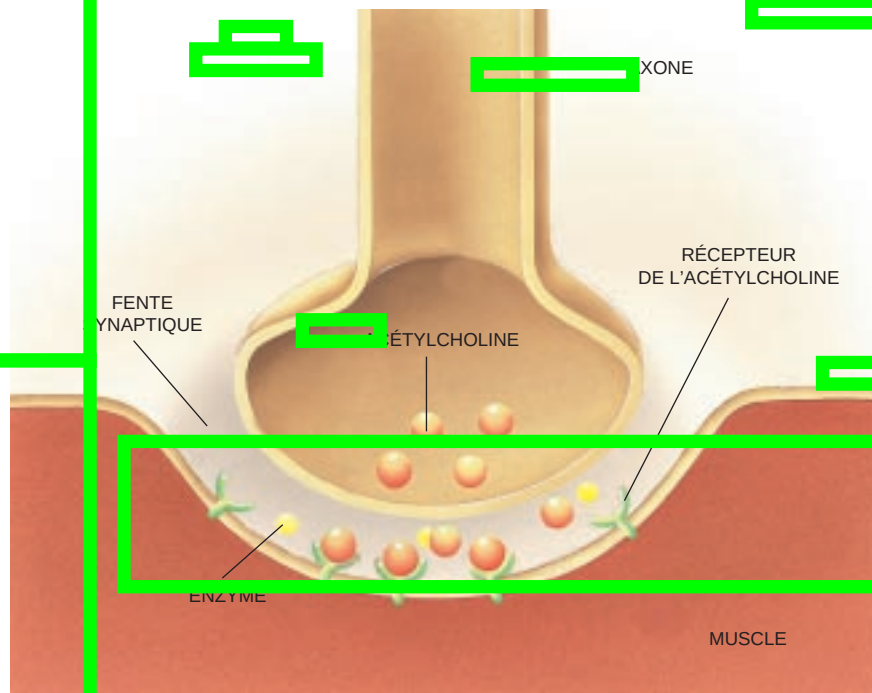
En outre, certains motoneurones de la corne antérieure, dans la moelle épinière des rescapés de la poliomyélite, sont anormalement petits. Ces neurones auraient été endommagés pendant l'infection aiguë et seraient plus fragiles. Normalement, les premiers signes d'épuisement des motoneurones n'apparaissent pas chez les personnes de moins de 60 ans. Comme le nombre de motoneurones des rescapés de la poliomyélite est réduit, la perte de seulement quelques unités motrices fonctionnelles semble réduire notablement la force musculaire.

Toutefois, le vieillissement n'est pas l'unique cause de l'épuisement des motoneurones dans le syndrome postpolio. On soupçonne que le virus de la poliomyélite subsiste dans le corps ou, plus précisément, que des particules virales, dormantes pendant plusieurs années, sont réactivées par un mécanisme inconnu : on a retrouvé des molécules d'ARN qui ressemblent à de l'ARN viral dans le liquide céphalo-rachidien et dans la moelle épinière de certaines personnes atteintes du syndrome postpolio, mais ces molécules sont absentes des anciens malades qui ne présentent pas le syndrome. Ces molécules d'ARN ne semblent pas être infectieuses, et l'on ignore si elles révèlent que le virus est en cause. On a également supposé que des anomalies immunitaires, des déficits hormonaux ou des intoxications par des molécules de l'environnement sont à l'origine du syndrome postpolio.

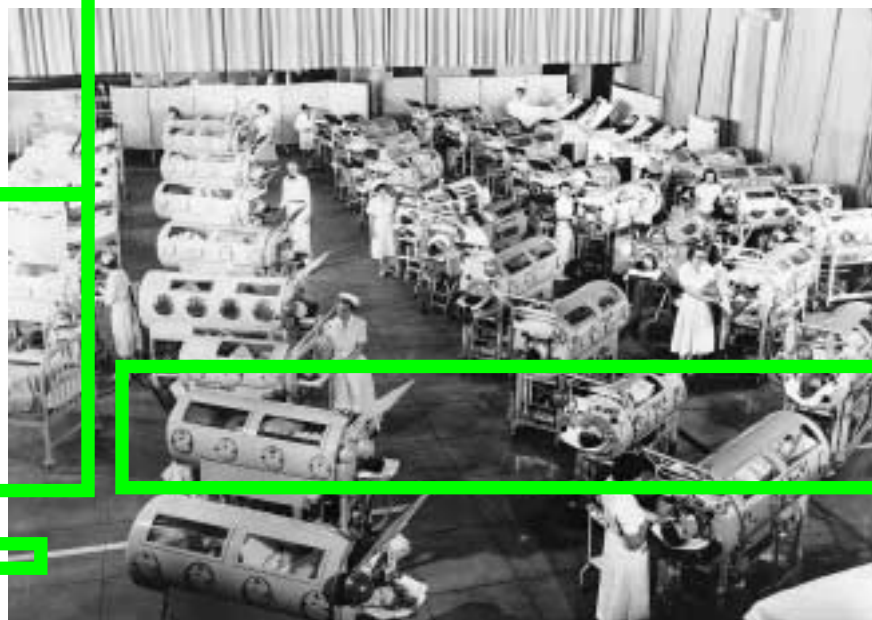
On ne dispose d'aucun test diagnostique du syndrome postpolio. Les analyses de sang, les biopsies musculaires et les enregistrements de l'activité musculaire révèlent les mêmes anomalies chez tous les rescapés de la poliomyélite, qu'ils aient ou non un syndrome postpolio. On diagnostique ce syndrome quand on a éliminé toutes les autres causes possibles.

L'apparition d'une faiblesse musculaire, après plusieurs années de stabilité, est sans doute le symptôme le plus caractéristique d'un syndrome postpolio, mais certains symptômes sont si généraux qu'il est souvent difficile d'exclure toutes les autres causes

possibles. Ainsi, une faiblesse musculaire peut résulter simplement d'un manque d'entraînement des muscles. La faiblesse musculaire due à l'inactivité peut évoquer un syndrome postpolio et le compliquer. Quelle qu'en soit la cause, la faiblesse risque de



3. L'ACÉTYLCHOLINE est le neurotransmetteur de la contraction musculaire. Lorsque l'acétylcholine est libérée par un axone dans une fente synaptique, elle se lie à ses récepteurs, sur la cellule musculaire, qui se contracte. Une enzyme dégrade l'acétylcholine présente dans la fente synaptique, en choline et en acétate, qui sont réabsorbés par l'axone et réassemblés en nouvelles molécules d'acétylcholine. Toute perturbation chronique de ce cycle se traduit par une faiblesse musculaire progressive.



4. LES «POUMONS D'ACIER» et les lits à bascule furent regroupés dans les hôpitaux lors des épidémies de poliomyélite des années 1950, afin que les infirmières et les médecins puissent surveiller plusieurs malades en même temps. Aujourd'hui, tous les hôpitaux ont des unités de soins intensifs, et les malades qui nécessitent des soins identiques sont regroupés : ces techniques sont héritées des épidémies de poliomyélite.

déclenche une cascade d'autres symptômes, qui masquent celui qui en est la cause.

Comme avec d'autres maladies chroniques, les médecins cherchent d'abord à soulager les symptômes, à améliorer le fonctionnement musculaire et à augmenter le bien-être de leurs malades. Selon les cas, ils prescrivent l'usage d'une canne ou d'un fauteuil roulant ou d'une assistance respiratoire. On encourage les malades à rester actifs aussi longtemps que possible. Parfois, des programmes d'exercices physiques sont recommandés ; parfois aussi, de simples étirements ou des séances de yoga s'imposent. Ainsi certains malades réussissent-ils à maintenir, voire à améliorer leur force musculaire.

Bien qu'il n'y ait pas de remède miracle, certains médicaments sont utiles : par exemple, de faibles doses d'antidépresseurs tricycliques soulagent parfois certaines douleurs, et la

pyridostigmine réduit la fatigue et améliore la force musculaire.

Généralement, le syndrome progresse lentement, et le pronostic global est bon, sauf en cas de difficultés pour respirer ou pour degainer. Néanmoins, lorsque l'état général est mauvais, un changement minime dans la stabilité des motoneurons risque de réduire de façon drastique la fonction musculaire, ce qui a souvent un effet psychologique dévastateur.

L'héritage individuel

La plupart des rescapés de la poliomyélite ont lutté : après le brusque déclenchement de la paralysie, ils ont progressivement récupéré à force de volonté et, pour beaucoup, repris une vie active, cherchant à oublier la maladie.

La plupart d'entre eux ont mené leur vie, ce qu'ils ont perdu, ce que

leur vie aurait pu être sans la maladie. L'exemple le plus célèbre est celui de Franklin Roosevelt : bien qu'il ait retrouvé assez rapidement l'usage de ses bras après la phase aiguë de la maladie, il a passé de nombreuses années à essayer, en vain, de réapprendre à marcher. Même après son élection, il faisait d'énormes efforts pour cacher son infirmité. Vers la fin de sa vie, sa faiblesse musculaire s'aggrava, vraisemblablement à cause d'un syndrome postpolio.

Pendant longtemps, la plupart des rescapés de la poliomyélite ont voulu éviter les autres rescapés et les groupes de soutien aux malades atteints de la maladie. Nous nous considérons comme des handicapés, mais pas comme des infirmes. En entraînant les muscles qui restaient, nous pensions que nous pourrions tout faire, y compris devenir président, comme Roosevelt.

La poliomyélite en France

Aujourd'hui, la poliomyélite est une maladie presque oubliée en France. Pourtant, dans les années 1950, elle y faisait environ cinq victimes par 100 000 habitants, dépassant même 4 000 cas, en 1957. Une personne atteinte sur dix mourait. Grâce à une vaccination intensive depuis les années 1960, la poliomyélite a été pratiquement éliminée des pays industrialisés et son éradication mondiale est en bonne voie. Malgré cette perspective encourageante, cette maladie reste un important problème de santé publique dans plusieurs pays en développement, notamment en Afrique et en Asie. De plus, des épidémies réapparaissent même dans des pays où elle semblait maîtrisée depuis longtemps. Ainsi, une épidémie a touché les Pays-Bas, en 1992, et l'Albanie, en 1996 (plus d'une centaine de cas).

De surcroît, un syndrome postpolio survient parfois 30 à 40 ans après l'infection aiguë chez près de la moitié des personnes ayant eu une poliomyélite très grave. La persistance du poliovirus dans le système nerveux central est l'une des hypothèses qui pourraient expliquer l'origine de ce syndrome. Ainsi, une équipe anglaise a trouvé des anticorps anti-poliovirus dans le liquide céphalo-rachidien de la majorité des personnes atteintes de syndrome postpolio (des antigènes de poliovirus auraient stimulé peu avant le système immunitaire). Par ailleurs, dans ce même liquide, trois groupes indépendants (américain, anglais et français) ont découvert la présence de séquences d'ARN de poliovirus (ou de virus apparentés).

Pour étudier la capacité du poliovirus à établir des infections persistantes, nous avons mis au point plusieurs modèles : des cultures de cellules et un modèle animal. Nous avons d'abord montré que le poliovirus

peut établir une infection persistante dans des lignées de cellules humaines d'origine neuronale. Plus récemment, nous avons utilisé des souches de poliovirus qui provoquent une poliomyélite chez la souris : elles attaquent les motoneurons de l'animal, créant des paralysies. Nous avons montré que le poliovirus persiste longtemps après la fin de la phase aiguë dans le système nerveux central des souris atteintes de poliomyélite. Ainsi, le poliovirus peut établir, chez la souris, une infection persistante dans le système nerveux central, en se multipliant à bas bruit.

Ce modèle animal nous a également appris qu'au cours de l'infection du système nerveux central par le poliovirus, les motoneurons sont détruits par un mécanisme de suicide cellulaire, nommé apoptose. On a longtemps pensé que les cellules infectées par le poliovirus étaient détruites uniquement par un phénomène de nécrose résultant de la multiplication des particules virales. Or nous avons montré que l'infection des motoneurons par le poliovirus active des signaux qui déclenchent l'apoptose.

Si les modèles animaux sont précieux pour la compréhension des pathologies humaines, ils ont leurs limites : la durée de vie de l'animal est limitée et les symptômes sont difficiles à évaluer. En revanche, bien que l'on ne puisse déduire des résultats obtenus sur les souris que le poliovirus persiste chez l'homme, nous poursuivons les recherches pour savoir si la persistance d'éléments viraux dans le système nerveux central contribue au développement du syndrome postpolio.

Bruno BLONDEL, Thérèse COUDERC,
Florence COLBÈRE-GARAPIN – Institut Pasteur

Plus tard, lors de la réapparition de la faiblesse, liée au syndrome postpolio, le refus est toujours aussi marqué : on ne comprend pas, on n'accepte pas. Colère, amertume, désespoir se succèdent. Heureusement, plusieurs associations de soutien ont été créées.

Pour beaucoup de rescapés de la poliomyélite, l'exercice est devenu une obsession quotidienne ; pour d'autres, c'est presque une dévotion. Les anciens poliomyélitiques ont appris à maîtriser leurs muscles et leurs mouvements. Cette leçon viscérale a des répercussions sur d'autres aspects de leur vie, ce qui explique probablement qu'ils réussissent leurs études ou leur travail.

En moyenne, ces personnes ont fait plus d'études que la population générale, se sont mariées et ont assumé les mêmes responsabilités familiales que les personnes non handicapées. Elles se sont mieux insérées dans le milieu professionnel que d'autres personnes handicapées, et ce sont parfois les plus atteintes, appareillées avec des béquilles, se déplaçant en fauteuil roulant ou reliées à une assistance respiratoire portative, qui ont atteint les plus hautes responsabilités.

L'héritage social

Le vaccin contre la poliomyélite est un succès médical. Des millions d'Américains ont d'abord fait du porte à porte pour collecter des fonds, puis accepté que leurs enfants soit vaccinés lors du premier grand essai du vaccin Salk, en 1954. Les recherches qui ont abouti à la mise au point du vaccin ont simultanément contribué à développer la virologie et l'immunologie.

De surcroît, les épidémies de poliomyélite ont accéléré le développement de la rééducation, dont l'objectif n'est pas la guérison ou la réparation des organes malades, mais la restauration des fonctions motrices et l'apprentissage des gestes qui assureront aux malades une vie autonome. Les techniques mises au point, il y a plusieurs dizaines d'années, pour aider les personnes ayant eu la poliomyélite, sont utilisées aujourd'hui pour les victimes de traumatismes crâniens ou de lésions de la moelle épinière, d'accidents vasculaires cérébraux et de maladies neurodégénératives.

Les unités de soins intensifs dont sont aujourd'hui équipés les hôpitaux sont également héritées des épidémies



5. LE PRÉSIDENT AMÉRICAIN Franklin Roosevelt a eu la poliomyélite en 1921. Ayant observé que des séances de natation dans les eaux chaudes naturelles de Warm Springs renforçaient ses muscles, il subventionna une fondation pour les personnes atteintes de poliomyélite. Pourtant, toute sa vie, il s'efforça de cacher son infirmité au public.

de poliomyélite des années 1950. Lorsque le personnel soignant commença à être débordé par l'afflux des personnes qui nécessitaient une assistance respiratoire, les machines furent regroupées pour que quelques infirmières puissent les surveiller simultanément. De plus, des centres spécialisés furent créés pour traiter les patients les plus gravement atteints. Certains de ces centres servent aujourd'hui aux victimes de lésions de la moelle épinière.

Les épidémies engendrèrent un élan de solidarité : des voisins apportaient de la nourriture aux familles mises en quarantaine chez elles, des

clubs d'adolescents collectaient de l'argent pour aider leurs camarades de classe hospitalisés, et des groupes de soutien furent créés.

Puis, quand les vaccins apparurent, la poliomyélite tomba dans l'oubli, ainsi que ses rescapés. Naguère considéré comme des exemples d'héroïsme, des milliers de survivants de la poliomyélite qui continuaient à avoir besoin d'aide médicale et financière furent laissés pour compte. Comme certains anciens combattants en ont fait l'expérience, la société n'aime pas qu'on lui rappelle ses morts et ses blessés.

Les vaccins eux-mêmes n'ont pas que des avantages : le vaccin oral de Sabin confère à la muqueuse digestive une immunité locale qui s'oppose à toute infection de la personne vaccinée. Malheureusement, s'il est plus efficace que le vaccin injectable de Salk, il déclenche, chaque année, la maladie qu'il devrait prévenir chez quelques personnes : les souches atténuées ont tendance à acquérir, dans l'intestin de la personne vaccinée, des mutations qui lui restituent parfois sa virulence et sont à l'origine des rares cas de poliomyélite associés à la vaccination. La maladie se déclare alors soit chez les personnes vaccinées pour la première fois qui ont un déficit immunitaire (le virus atténué se multiplie et finit par entraîner une paralysie), soit chez les personnes qui vivent à leur contact sans être elles-mêmes immunisées. Aujourd'hui, on recommande deux premières vaccinations par injection du virus tué, suivies, quelque temps après, par deux rappels avec le vaccin oral contenant le virus vivant atténué.

Lauro HALSTEAD est professeur à la Faculté de médecine de Georgetown. Il dirige les programmes d'étude du syndrome postpolio et des lésions de la moelle épinière à l'Hôpital de Washington, destiné à la rééducation.

Post-Polio Syndrome, sous la direction de Lauro S. Halstead et Gunnar Grimby, Hanley & Belfus, Philadelphie, 1995.

Tony GOULD, *A Summer Plague : Polio and Its Survivors*, Yale University Press, 1995.

N. PAVIO, M.-H. BUC-CARON et F. COLBÈRE-GARAPIN, *Persistent Poliovirus Infection of Human Fetal Brain Cells*, in *Journal of Virology*, vol. 70, pp. 6395-6401, 1996.

Daria A. TROJAN et Neil R. CASHMAN, *Current Trends in Post-Poliomyelitis Syn-*

drome, Milestone Medical Communications, New York, 1996.

Kathryn BLACK, *In the Shadow of Polio : A Personal and Social History*, Addison-Wesley, 1996.

J. DESTOMES et al., *Persistent Poliovirus Infection in Mouse Motoneurons*, in *Journal of Virology*, vol. 71, pp. 1621-1628, 1997.

Managing Post-Polio : A Guide to Living Well with Post-Polio Syndrome, sous la direction de Lauro S. Halstead, NRH Press et ABI Professional Publications, Falls Church, Va., 1998.

D'autres références bibliographiques et des informations sur les associations d'entraide sont disponibles sur le site <http://www.pourlascience.com>

Les kangourous carnivores

STEPHEN WROE

À l'opposé des kangourous et des koalas actuels, certains marsupiaux australiens ont été de redoutables prédateurs.

1. UN RAT-KANGOUROU GÉANT aux dents puissantes (*Ekaltadeta ima*) bondit sur un jeune mammifère dans la forêt tropicale. Deux «lions» marsupiaux (*Wakaleo vanderleuri*) et un oiseau terrestre géant (*Bullockornis planei*) assistent à cette scène, qui se déroule au Miocène, il y a environ 15 millions d'années. Eux aussi auraient pu se nourrir de mammifères.



Il y a 15 millions d'années, au Nord-Est de l'Australie, une famille de petits mammifères émerge des buissons, enve-

lue par la chaleur du soleil. Les oreilles de ces animaux pivotent sans cesse, attentives au moindre craquement suspect : boire est toujours une activité dangereuse. Soudain, une silhouette sombre et puissante surgit d'un fourré ; d'un bond, elle est sur un des jeunes, emplant sa victime sur deux longues dents effilées comme une dague, puis elle emporte sa proie pour s'en repaître tranquillement. Cette banale scène de prédation ne devient remarquable que si l'on précise que le prédateur est un kangourou : un rat-kangourou géant, aux dents puissantes (*Ekaltadeta ima*).

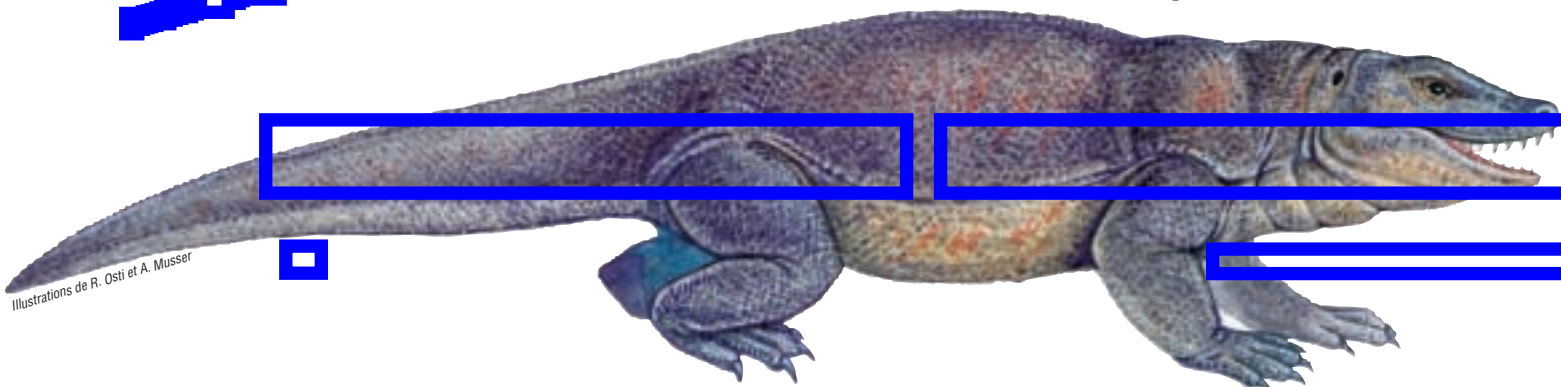
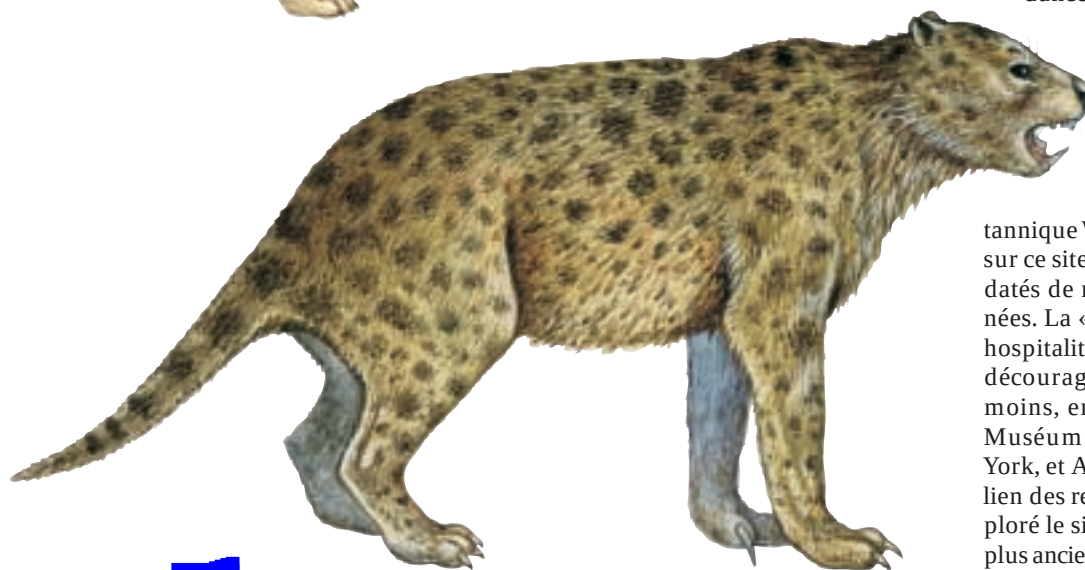
Aujourd'hui, en Australie, les préda-

sang chaud sont rares : ce sont le «chat» marsupial (*Dasyurus maculatus*) et le diable de Tasmanie (*Sarcophilus harrisii*). Le dingo, un chien sauvage, a été introduit par l'homme il y a seulement 4 000 à 5 000 ans. Le «chat» marsupial, semblable aux

chats placentaires, pèse jusqu'à sept kilogrammes. Marsupial également, le diable de Tasmanie ressemble à un chien avec une tête de hyène. Il dévore des carcasses entières, jusqu'aux dents. Avec d'autres «chats» marsupiaux, ainsi que des souris marsupiales insectivores, ces deux animaux composent la famille des Dasyuridés.

Les paléontologues ont souvent supposé qu'aucun groupe de grands carnivores à sang chaud n'a vécu en Australie. Récemment, Tim Flannery, à l'Université Harvard, a montré que le sol pauvre et les climats irréguliers des derniers 10 millions d'années ont avantage les prédateurs à sang froid, tel *Megalanias prisca*, un lézard de 5,5 mètres de long qui vivait au Pléistocène. Ce varan est l'ancêtre du dragon de Komodo. Voir *Les dragons de Komodo*, Claudio Cofi, *Pour la Science*, mai 1999). Les prédateurs à sang froid ont besoin de moins de nourriture que ceux à sang chaud, de sorte qu'ils sont mieux adaptés aux milieux où la taille et l'abondance des proies sont limitées par une faible biomasse végétale. Cependant, un fossile récemment découvert à Riversleigh, dans le Queensland, remet en cause cette hypothèse.

En 1900, le naturaliste britannique W.E. Cameron avait découvert sur ce site reculé des fossiles qu'il avait datés de millions d'années. La «jeunesse» de ces fossiles et l'hospitalité de la région ont longtemps découragé les paléontologues. Néanmoins, en 1963, Richard Tedford, du Muséum d'histoire naturelle de New York, et Alan Lloyd, du Bureau australien des ressources minérales, ont réexploré le site et y ont trouvé des fossiles plus anciens et plus extraordinaires qu'ils ne pensaient en découvrir.

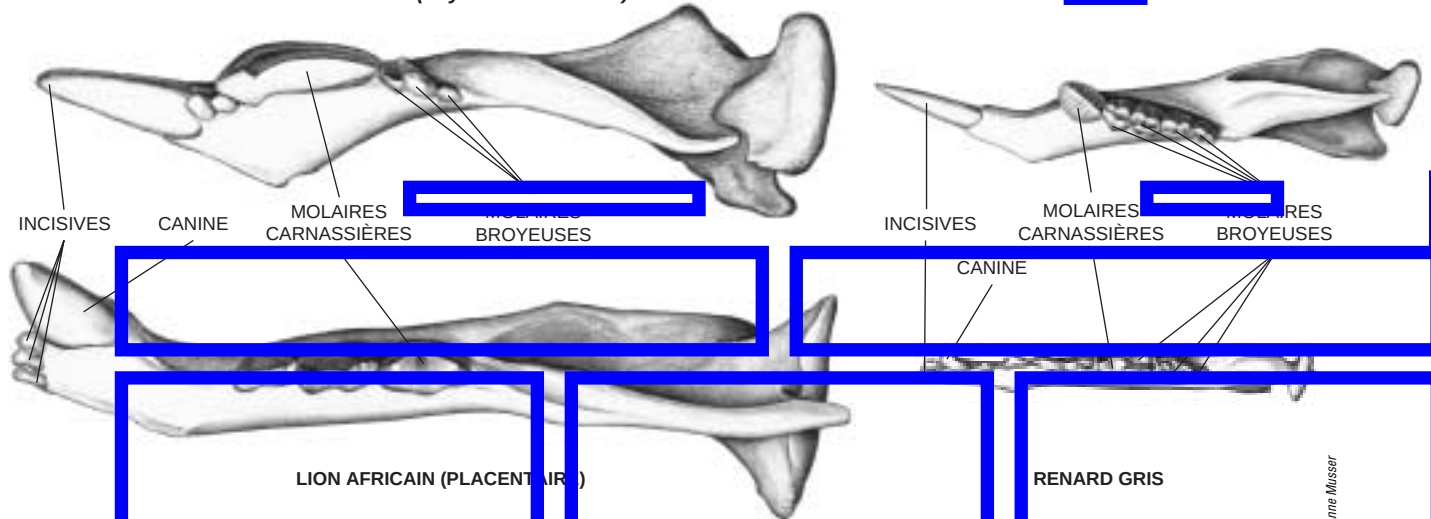


2. PARMI LES GRANDS CARNIVORES disparus du continent australien, on trouvait (de haut en bas) le rat-kangourou géant (*Ekaltadeta ima*) d'environ 20 kilogrammes, le loup marsupial (*Thylacinus*

potens) de 45 kilogrammes, le lion marsupial (*Thylacoleo carnifex*) qui pesait jusqu'à 260 kilogrammes, et le varan géant (*Megalanias prisca*) dont le poids dépassait 600 kilogrammes.

LION MARSUPIAL (*Thylacoleo carnifex*)

RAT-KANGOUROU GÉANT



3. LES CARNASSIÈRES, des molaires aiguisées en lames verticales tranchantes, sont la marque des prédateurs terrestres. Les mammifères placentaires carnivores et les marsupiaux carnivores spécialisés n'ont, sur chaque mâchoire, qu'une seule dent aussi nommée

pour cette tâche. Les molaires en arrière de cette dent sont réduites ou perdues. Les carnivores moins spécialisés, placentaires ou marsupiaux, qui consomment plus de végétaux, conservent leurs molaires broyeuses en arrière des carnassières.

Leurs découvertes ont suscité d'autres expéditions. En 1983, Michael Archer, qui dirige aujourd'hui le Muséum de Sydney, a fait une découverte inattendue... en se penchant seulement un peu : assis sur un gros bloc de rocher pour se reposer, il a regardé à ses pieds et a ainsi trouvé un bloc qui contenait des os inconnus de mammifères du Tertiaire australien (de -65 millions à -1,8 million d'années) qu'il n'en a été décrit au cours des siècles précédents. Depuis, les découvertes, notamment celles de gros carnivores et d'autres animaux, ont été nombreuses. Quelques fossiles de gros carnivores sont en excellent état.

Les os de la plupart de ces animaux, qui semblent avoir été piégés dans des grottes calcaires où l'eau riche en carbonate de calcium les a rapidement et parfaitement préservés, indiquent que les anciens carnivores d'Australie diffèrent de ceux d'aujourd'hui. Depuis 1985, avec les neuf nouvelles espèces de Riversleigh, le bestiaire des grands carnivores australiens âgés d'au moins cinq millions d'années est composé de deux sortes de « loups » marsupiaux, de cinq espèces de « lions » marsupiaux et d'un « chat » marsupial.

Les rats-kangourous géants sont apparentés au rat-kangourou musqué actuel (voir la figure 4), qui ressemble à un rat et se nourrit de plantes et de petits animaux. Le rat-kangourou musqué pèse moins de un kilogramme.

Seul parmi les kangourous à ne pas sauter, il est le dernier représentant d'une famille qui comprenait quelques individus redoutables. Les rats-kangourous géants pesaient 15 à 60 kilogrammes et, comme leurs descendants minuscules, ils marchaient sur leurs quatre pattes.

Ces loups marsupiaux (thylacinidés), les chats (dasyuridés) et les lions marsupiaux (thylacoléonidés), ainsi nommés en raison de leurs ressemblance avec les canidés et les félidés, sont néanmoins apparentés aux kangourous. Le dernier des loups marsupiaux, le loup de Tasmanie, a été exterminé au début du 20^e siècle. Il était supposé tuer les moutons. Les chats et les lions marsupiaux, avec un crâne court, large et plat, occupaient probablement une niche écologique similaire. Bien qu'aucun fossile ne conserve de traces d'une poche marsupiale, les os indiquent que ces créatures étaient des marsupiaux.

Une forêt redoutable

Pendant une grande partie du Miocène (il y a 25 à 5 millions d'années), les forêts couvraient entièrement l'Australie. Elles abritaient une faune très variée, avec, notamment, des rats-kangourous géants, armés de dents puissantes.

Cet animal est l'un des plus anciens rats-kangourous (cinq autres espèces provenant de dépôts plus récents ont été décrites). Il pesait 10

à 20 kilogrammes, et les fossiles de deux crânes presque complets témoignent de sa puissance.

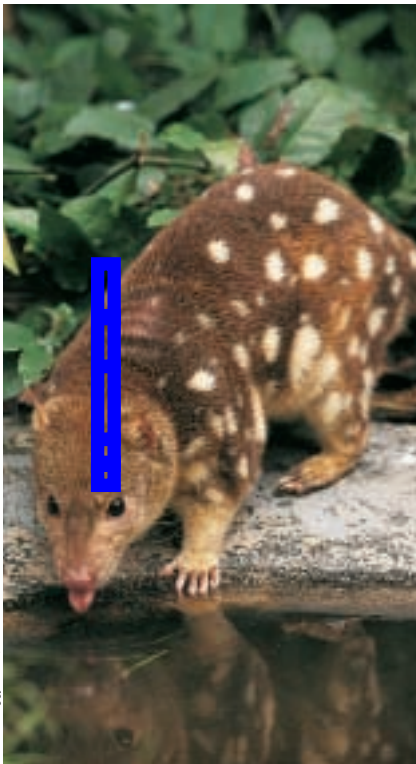
Contrairement à une idée reçue, les mammifères terrestres carnivores se reconnaissent à la présence de dents jugales (dans la joue) tranchantes, plutôt qu'à de longues canines : de nombreux ours humains consomment de la viande avec des petites canines, alors que les grilles, végétariens, en ont de grandes.

Les deux à quatre dernières dents des mâchoires des rats-kangourous géants, des lions marsupiaux et des carnivores placentaires les moins spécialisés sont des molaires broyeuses.

qui, chez leurs ancêtres herbivores, broyaient les végétaux. En avant de ces molaires, des dents coupantes nommées carnassières (voir la figure 3) tranchent efficacement le muscle, la peau et les tendons des proies. Dans ces groupes d'animaux, les espèces les plus carnivores ont des carnassières développées, mais des molaires réduites, voire perdues.

L'importance des carnassières d'un animal révèle ainsi la proportion de chair de son alimentation. Par exemple, la mâchoire d'un rat-kangourou rap-

porteur opportuniste : les molaires antérieures sont tranchantes, mais les molaires postérieures conservent une importante capacité à écraser. Cependant l'architecture robuste du crâne d'*Ekaltadeta ima* indique un cou massif et des muscles de la mâchoire puissants, nécessaires à la prédation. En revanche, aucune longue canine ne s'est



développées. Ce sont les incisives inférieures qui sont devenues des lames acérées.

Selon certains paléontologues, les rats-kangourous géants mangeaient de la viande seulement lorsqu'elle était disponible, et ils complétaient leur régime par des végétaux. Ces kangourous atypiques ont terrorisé le continent australien pendant au moins

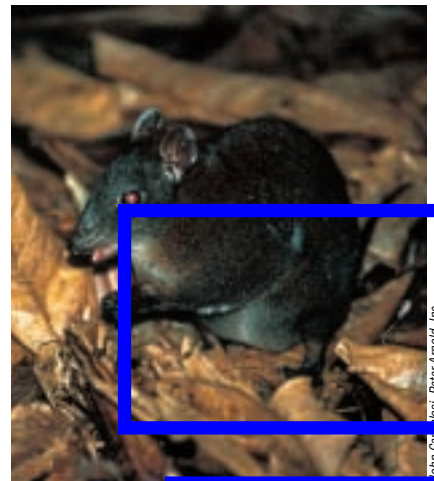
25 millions d'années et se sont éteints au cours des derniers 40 000 ans.

D'autres surprises

Les branches basses abritaient d'autres prédateurs redoutables : les lions marsupiaux. Ils ont également évolué à partir d'un paisible herbivore. Les espèces les plus primitives ont des molaires non spécialisées, typiques des omnivores, ainsi que des lames carnassières. Chez d'autres espèces, les molaires broyeuses sont réduites ou perdues, et les carnassières sont devenues énormes.

Aujourd'hui, les paléontologues s'accordent à dire que les lions marsupiaux (certains ont pourtant supposé qu'ils ne pouvaient manger que des aliments mous, tels les melons!) considéraient que l'espèce la plus récente, *Thylacoleo carnifex*, était un marsupial carnivore très adapté. Sans dents broyeuses ni canines, il utilisait ses redoutables carnassières et ses longues incisives.

Thylacoleo carnifex est le seul marsupial dont on connaisse le squelette complet. De nombreux paléontologues supposent qu'il avait la taille d'un léopard, mais la robustesse du squelette me semble indiquer que cet animal pouvait être aussi lourd qu'un lion actuel, puissant et peu endurant, avec des membres antérieurs très musclés. Ses dents tranchantes et ses griffes



4. LES MINUSCULES DESCENDANTS
Les grands prédateurs australiens du Miocène ne manquent pas de férocité. Le diable de Tasmanie (à gauche) et le chat marsupial (en haut, à gauche) sont des dasyuridés ; le rat-kangourou musqué (ci-dessus) est le dernier descendant des rats-kangourous géants qui terrorisaient les forêts il y a 15 millions d'années.

gainées, tel un couteau à cran d'arrêt, à l'extrémité de chaque pouce opposable, lui permettaient de capturer des proies probablement plus grosses que lui. *Thylacoleo carnifex* a vécu jusqu'à il y a 50 000 ans environ : il s'est peut-être nourri d'arbres.

De la taille d'un léopard, les lions marsupiaux du genre *Wakaleo* étaient plus petits. Ces animaux et, peut-être aussi, les espèces du genre *Thylacoleo*, semblent avoir chassé à partir des branches d'arbres, comme les léopards. De la taille d'un chat domestique, *Priscileo roskeleyae* chassait surtout des proies arboricoles.

Lorsque les Européens sont arrivés en Australie, il y a plus de 200 ans, ils n'ont trouvé que deux familles de marsupiaux carnivores : le loup de Tasmanie, seul survivant des loups marsupiaux, et le groupe des dasyuridés, dont le poids n'excédait pas un kilogramme. Plus de 60 espèces de ces animaux vivent encore aujourd'hui.

Les paléontologues pensaient que les dasyuridés, une famille actuelle très diversifiée de marsupiaux insectivores et carnivores, étaient beaucoup plus courants que les thylacinidés dans le passé. Ils se trompaient : depuis 1990, avec la découverte de «loups» du Miocène découverts, neuf thylacinidés sont connus et quatre autres espèces sont en cours de description. En revanche, dans les dépôts du Miocène, une seule espèce de dasyuridés a été décrite : la proportion de lions marsupiaux et de dasyuridés pendant le Miocène était opposée à celle d'aujourd'hui.

Le loup marsupial le plus connu, ressemblait à la plupart des canidés : il était complètement terrestre, possédait un long museau et se nourrissait de proies beaucoup plus petites que lui. Cependant, il était peu adapté à la course, ne chassait pas en meute et avait des dents adaptées à un régime exclusivement carnivore.

Chez les dasyuridés, la conformation des dents est différente de celle des thylacinidés carnivores. Chaque molaire conserve la possibilité de broyer, tout en pouvant trancher verticalement : les plus spécialisés (celle des thylacinidés) ont des surfaces broyeuses réduites, tandis que le tranchant vertical est développé.

Tous les loups marsupiaux étaient carnivores (les plus petits, moins

spécialisés, étaient aussi insectivores), mais tous n'avaient pas un profil de canidés. Certains «loups» du Miocène étaient petits par rapport au loup de Tasmanie, et l'un d'entre eux, *Wabulacoleo*, était peut-être un

Les thylacinidés étaient-ils tous terrestres? Les fragments de crânes et de mâchoires dont on dispose sont insuffisants pour répondre. Néanmoins, le spécimen âgé de 15 millions d'années découvert récemment à Riversleigh, dont le crâne et la majeure partie de la mandibule ont été conservés, vivait sur la terre ferme.

Avec Henk Godthelp, de l'Université de Nouvelle-Galles du Sud, et M. Archer, j'ai découvert à Murgoo, dans le Sud-Est du Queensland, un marsupial de la taille d'une souris qui

vivait il y a 55 millions d'années. Sa dentition primitive, non spécialisée, rend son parenté avec les autres marsupiaux difficile à établir. Il serait un ancêtre des thylacinidés et des dasyuridés, ou de tous les marsupiaux australiens, ou encore une nouvelle espèce apparentée aux Ameridelphia, groupe taillé pour l'Amérique du Sud, plutôt qu'à l'Australidelphia. L'Antarctique joignait autrefois l'Amérique du Sud et l'Australie en un continent géant appelé Gondwana. Selon certains paléontologues, seuls les Australidelphia ont pénétré en Australie avant que le Gondwana ne se disloque. Les



5. LE CRÂNE FOSSILISÉ du rat-kangourou géant aux dents puissantes redoutables et des carnassières crénelées, qui devaient lui permettre de tuer et de dévorer ses proies.

Un oiseau tueur?

En novembre 1998, Peter Murray et Kirk Megirian, du Muséum d'histoire naturelle d'Adélaïde, ont décrit et reconstitué un oiseau terrestre disparu nommé *Bullockornis planei*. Il est de la famille australienne des dromornithidés, décrite pour la première fois en 1839. Apparentés à des oiseaux principalement herbivores, ces animaux pesaient jusqu'à 500 kilogrammes. La plupart des paléontologues pensaient qu'ils étaient aussi herbivores, mais la reconstitution de *Bullockornis planei* montre une tête massive de près de 50 centimètres de long, munie d'attaches musculaires énormes. Que mangeait un



oiseau avec de tels muscles masticateurs et un bec assez grand pour cacher un ballon de rugby?

En 1991, Lawrence Witmer, de l'Université de l'Ohio, et Kenneth Rose, de l'Université Johns Hopkins, ont démontré que le bec massif et la musculature des mâchoires de *Diaryma*, un oiseau éteint d'Amérique du Nord et d'Europe, indiquait un régime carnivore. J'ai donc supposé que certains dromornithidés se nourrissaient aussi de viande. Les dromornithidés ont alors été les plus gros carnivores bipèdes depuis la disparition des dinosaures carnivores.

La diversité des mammifères

Un mammifère est un animal à sang chaud, généralement placentaire, qui se reproduit vivipare et allaite ses petits. Au-delà de cette définition, les mammifères sont divisés en trois grands groupes : les monotrèmes, les marsupiaux ou métathériens, et les placentaires ou euthériens. Ces trois ordres cohabitent uniquement sur le continent australien et en Nouvelle-Guinée.

Les monotrèmes, représentés en Australie par l'ornithorynque (voir la figure 1) et par un échidné (une sorte de gros hérisson au museau allongé), associent des caractères reptiliens et mammaliens. Un orifice, nommé cloaque,



1. L'ornithorynque (*Ornithorhynchus anatinus*) est un monotrème. Il pond des œufs, mais allaite ses jeunes.



2. La larve du possum «queue en brosse» (*Trichosurus vulpucela*) rejoint la poche marsupiale où elle s'accroche à une mamelle.



3. Le veau (*Bos taurus*) est un mammifère placentaire : il est autonome dès la naissance.

commun aux voies génitales, urinaires et intestinales, ainsi que la reproduction ovipare rappellent les reptiles, alors que la présence de poils, l'allaitement des nouveau-nés et la température corporelle presque constante les rapprochent des mammifères. En revanche, des mâchoires incluses dans un bec corné constituent une caractéristique des monotrèmes.

Les mammifères marsupiaux et placentaires composent le groupe des thériens, c'est-à-dire des mammifères qui ne pondent pas d'œufs. Ils se distinguent des autres vertébrés, et, notamment, des monotrèmes, par la réduction du nombre des os de la paroi latérale du crâne au niveau de l'articulation de la mandibule : seule l'alisphénoïde et le squamosal assurent cette fonction chez les marsupiaux, alors qu'il y en a six chez les autres vertébrés.

Les marsupiaux et les placentaires se différencient par la croissance des jeunes. Les mammifères placentaires naissent lorsque leur développement est achevé (voir le jeune veau de la figure 3). Les marsupiaux, quant à eux, naissent à l'état de larves et passent les premiers mois de leur vie dans la poche marsupiale, nommée marsupium, de leur mère, où ils se nourrissent du lait des mamelles (voir la figure 2).

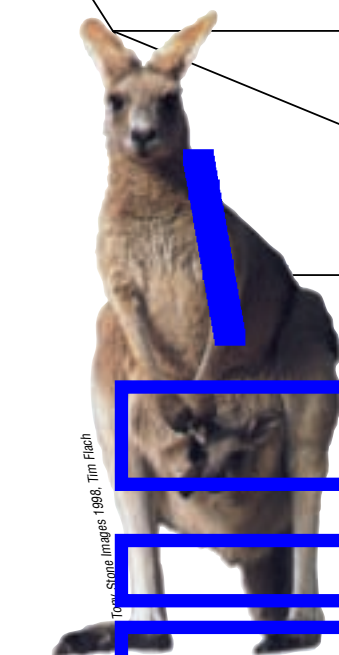
Le placenta est un organe aplati à l'interface des circulations maternelle et fœtale. Celui des mammifères placentaires est – leur nom est mérité – très développé. Toutefois, les marsupiaux ont également un placenta, mais plus simple et plus restreint.

Par ailleurs, la plupart des marsupiaux ont deux os, non pas os marsupiaux, au niveau du bassin, que les placentaires n'ont pas. Ces os sont situés à l'avant de la partie antérieure du bassin, soit libres. Contrairement à certaines hypothèses, ils ne dépendent pas de la présence du marsupium, mais servent plutôt de point d'ancrage à des muscles reliés aux membres postérieurs. L'os pénien, nommé baculum, et les cartilages vaginaux de certains placentaires, sont peut-être des structures homologues des os marsupiaux des métathériens. Après être devenu flottants, les os marsupiaux se sont soudés et ont formés le bassin.

Les euthériens ont une véritable dentition de lait qu'ils remplacent entièrement. En revanche, chez les marsupiaux, seule la troisième prémolaire (de chaque demi-mâchoire) est remplacée par une dent définitive. La formule dentaire des marsupiaux est donc : quatre ou cinq incisives par demi-mâchoire, trois pré-molaires et quatre molaires chez les marsupiaux, quatre incisives, quatre pré-molaires et trois molaires chez les placentaires.

Les marsupiaux et les placentaires sont apparus à la même période vers le milieu du crétacé. Les premiers ne constituent donc pas un stade intermédiaire entre les mammifères du début de l'ère secondaire et les placentaires. Ce sont deux groupes frères.

Jean-Yves CROCHET
Université de Montpellier 2



Tom Stone Images 1998, Tim Flach

6. ARBRE PHYLOGENIQUE des marsupiaux australiens. Pour chaque famille, un représentant est noté entre parenthèses. Les carnivores sont notés en rouge

- PERAMELETTIDÉS (péramèle)
- MICROBIOTIDÉS (colo-colo)
- DASYURIDÉS (chat marsupial)
- THYLACINIDÉS (loup marsupial)
- MYRMECOBIDÉS (numbat)
- NOTORYCTIDÉS (taupe marsupiale)
- PHASCOLANTHIDÉS (koala)
- THYLACOLECTIDÉS (lion marsupial)
- AUTRES VOMBATOMORPHIENS (wombat)
- MACROPODIDÉS (kangourou)
- POTOROÏDÉS (kangourou-rat)
- YPSIPRYMNODONTIDÉS (rat-kangourou géant)
- HALANGEROIDÉS (phalanger-renard)
- ETAUROIDÉS (possum à queue préhensile)

nouveaux fossiles découverts contredisent cette hypothèse.

Mort aux tueurs

Pourquoi les grands carnivores australiens ont-ils disparu alors qu'ils étaient nombreux et variés au Miocène? Le dernier des lions marsupiaux (*Thylacoleo carnifex*) et le dernier des rats-kangourous géants (*Propleopus oscillans*) vivaient encore lorsque les aborigènes sont arrivés en Australie, il y a au moins 50 000 ans. Les populations humaines ont-elles tué ces animaux?

La question reste ouverte. L'exemple du loup de Tasmanie, qui n'a pas survécu à l'introduction du dingo, semble mettre l'homme en cause, mais l'influence humaine sur les autres espèces est moins nette, car la diversité des marsupiaux carnivores déclinait déjà dans la seconde moitié du Miocène, bien avant l'arrivée des

hommes. Ainsi, au moins cinq loups marsupiaux vivaient au milieu du Miocène, deux coexistaient à la fin du Miocène, mais un seul a connu les hommes.

Les aborigènes ont-ils initié un processus d'extinction entamé par la sécheresse? Dès le milieu du Miocène, en effet, l'Australie subit des glaciations de plus en plus sévères, ainsi qu'une baisse des précipitations et du niveau des mers. Lors des deux derniers millions d'années, la faune australienne a connu 20 périodes glaciaires.

et à l'arrivée des hommes, les grands herbivores auraient disparu du continent. Sans proie, les marsupiaux prédateurs australiens se sont éteints. Des grands marsupiaux carnivores australiens et américains, seuls le «chat» marsupial et le diable de Tasmanie ont survécu : tâchons de protéger ces deux derniers tueurs à poche.

Stephen WROE est paléontologue à l'Université de Sydney.

M. ARCHER, S. HAND et H. GODTHELP, *Riversleigh: The Story of Animals in Ancient Rainforests of Inland Australia*, Reed Books, 1994.

S. WROE, *Killer Kangaroo*, in *Australasian Science*, vol. 19, n° 6, pp. 25-28, juillet 1998.

S. WROE, *The Geologically Oldest Dasyurid, from the Miocene of Riversleigh, Northwestern Queensland*, in *Palaeontology* (à paraître).

Le ciel infrarouge vu de l'espace

A. ABERGEL • F. BOULANGER • G. LAGACHE • E. DARTOIS • J.-L. PUGET

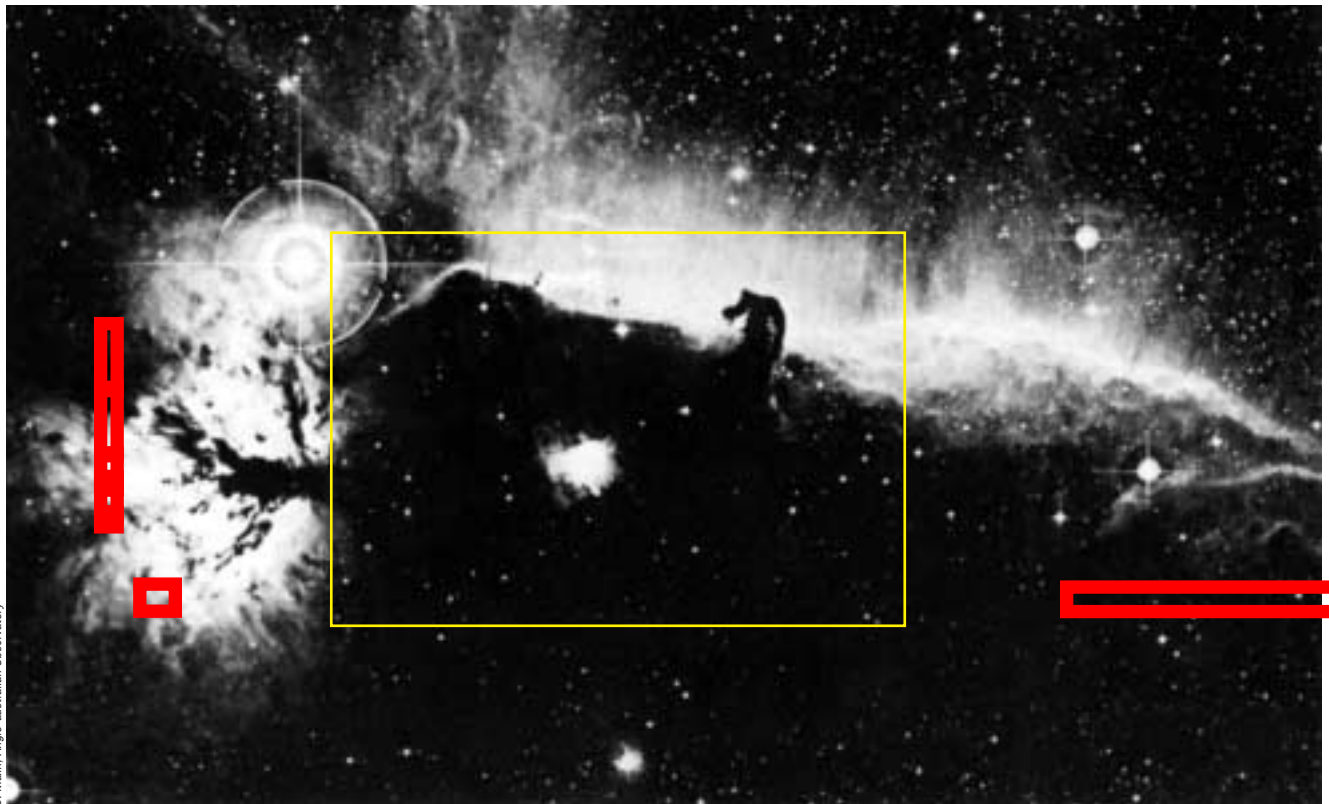
Le satellite ISO a déterminé la nature des poussières du milieu interstellaire et mesuré le rythme de formation des étoiles au cours de l'évolution de l'Univers.

L'atmosphère terrestre est quasi opaque aux rayonnements infrarouges. Dans les années 1970, les astronomes n'ont pu mesurer les émissions des corps célestes dans une grande partie du spectre d'onde. Les premières observations dans l'infrarouge, à partir du sol, étaient incomplètes, et l'utilisation d'avions, de ballons ou de fusées pose des problèmes techniques et logistiques considérables.

Les satellites artificiels ont permis aux astronomes d'envisager des observations longues, soit pour étudier le

ciel entier, soit pour détailler des régions spécifiques. Le premier satellite d'observation des rayonnements infrarouges, *IRAS* (pour *Infrared astronomical satellite*, c'est-à-dire «satellite astronomique infrarouge»), fut lancé par la NASA en 1983. Il dressa une carte complète du ciel à quatre longueurs d'onde : 12, 25, 60 et 100 micromètres (un micromètre est égal à un millionième de mètre ; les rayonnements infrarouges sont ceux dont la longueur d'onde est supérieure à 0,7 micromètre et inférieure au millimètre ; au-delà s'étend le domaine radio).

Le 7 novembre 1995, une fusée *Ariane 4* mit en orbite autour de la Terre le satellite *ISO* (*Infrared Space Observatory*, soit «observatoire spatial dans l'infrarouge») de l'Agence spatiale européenne. Il était équipé d'un gros cryostat, qui contenait initialement plus de 2 000 litres d'hélium liquide. Ce liquide cryogénique maintenait la température des instruments embarqués à trois kelvins environ (soit -270°C), évitant que le rayonnement infrarouge émis par les instruments à bord ne perturbe les mesures. L'autonomie du système



D. Malin, Anglo-australian Observatory

de refroidissement devait être de 18 mois, mais les astronomes ont eu la bonne surprise de voir le satellite fonctionner pendant 29 mois.

Le satellite était sur une orbite très elliptique avec un périégée de 1 000 kilomètres et un apogée de 78 500 km. La période de révolution était de 24 heures, mais les instruments ne fonctionnaient que 16 heures sur 24, les mesures étant impossibles durant la traversée des ceintures de Van Allen, zones où le champ magnétique terrestre canalise des particules solaires très énergiques, qui perturbent les détecteurs.

Le télescope collecteur a un diamètre de 30 centimètres, identique à celui du satellite *IRAS*. Quatre instruments sont à bord : deux spectromètres, un multi-photomètre (*ISOPHOT*) et une caméra nommée *ISOCAM*. Ainsi, *ISO* a mesuré les rayonnements électromagnétiques de longueurs d'onde comprises entre 2,5 et 240 micromètres. La résolution angulaire accessible étant égale à quelques secondes d'angle avec la caméra *ISOCAM*.

Si les opérations sur le satellite sont définitivement arrêtées (faute d'hélium pour refroidir le télescope), les mesures sont encore en cours de dépouillement. Déjà les premiers résultats modifient notre vision de

l'Univers. *ISO* a étudié les constituants du milieu interstellaire et éclairé l'histoire de la formation des étoiles dans l'Univers. Nous examinerons ici ces deux aspects.

Le milieu interstellaire

Lorsque l'on regarde l'Univers dans le domaine visible, le seul que les astronomes ont longtemps étudié, on voit essentiellement des étoiles. À la fin de leur vie, celles-ci éjectent, souvent violemment, des couches de gaz dans l'espace interstellaire : ainsi se constitue la matière interstellaire. Cette matière s'organise ensuite jusqu'à former de nouvelles étoiles, qui brillent, qui meurent et qui, à nouveau, recèdent leurs constituants dans l'espace. Les astrophysiciens explorent l'un des aspects de la formation de la matière interstellaire.

Sous quelle forme la matière interstellaire se trouve-t-elle ? Une partie est constituée de gaz, mais une autre est constituée de poussières. Ces dernières ont été découvertes par les astronomes parce qu'elles leur cachaient les étoiles (voir la figure 1) : c'est le phénomène d'extinction.

Les poussières interstellaires absorbent le rayonnement visible émis par les étoiles (l'absorption dépend fortement de la longueur d'onde). Les

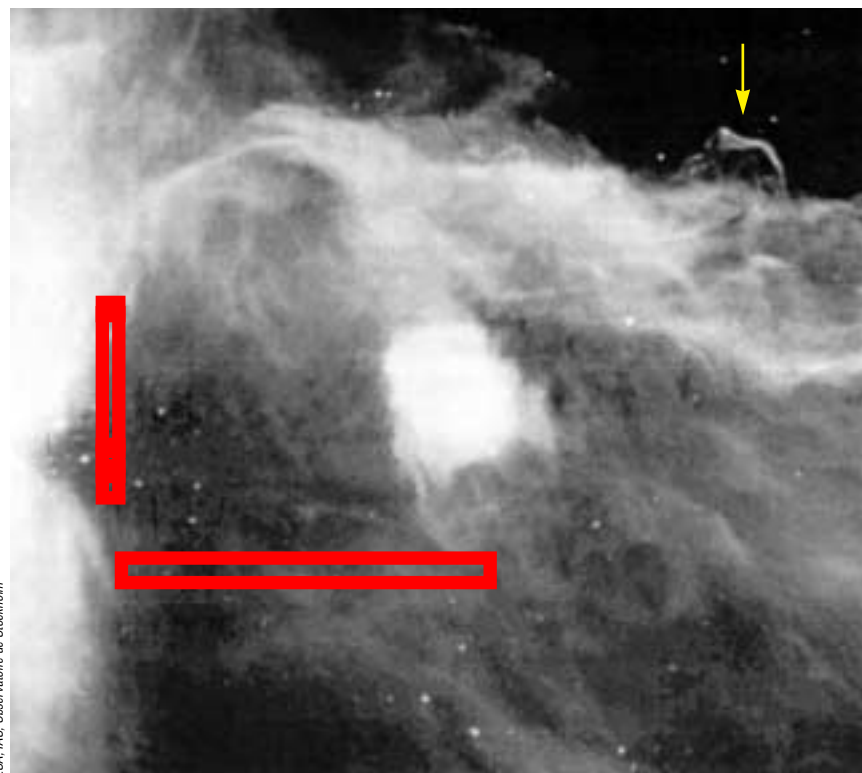
astronomes étudient les poussières en mesurant le rayonnement des étoiles qui traverse les vastes nuages de poussières.

En dispersant le rayonnement mesuré (à la manière de prismes dans le domaine visible), des systèmes optiques fabriquent ensuite des spectres. Ces spectres contiennent des pics d'absorption : l'intensité reçue devient très faible à certaines longueurs d'onde. Ces pics d'absorption sont dus aux vibrations de liaisons chimiques qui sont présentes dans les molécules qui composent les poussières.

Dans les années 1970, les premières mesures de l'émission infrarouge des poussières ont mis en évidence les pics d'absorption élargis, caractéristiques de liaisons chimiques de la matière interstellaire.

Un pic à une longueur d'onde égale à 9,7 micromètres a révélé la vibration de la liaison entre un atome de silicium et un atome d'oxygène. Une longueur d'onde de 18 micromètres correspondait à la modification de l'angle formé par un atome d'oxygène central lié à deux atomes de silicium.

Ces pics indiquaient la présence de silicates, c'est-à-dire des combinaisons d'oxydes métalliques et de silice. Par analogie avec les spectres obtenus en laboratoire pour divers



1. LES POUSSIÈRES INTERSTELLAIRES apparaissent dans le visible comme de vastes nuages sombres qui absorbent le rayonnement émis par les étoiles situées derrière elles (à gauche). En revanche, ces poussières brillent sur l'image infrarouge prise par le satellite *ISO* (l'image de droite représente un champ qui correspond au cadre jaune). Les points lumineux sur l'image dans l'infrarouge correspondent à des étoiles qui sont enfouies dans le complexe ou situées à l'extérieur. Au cœur du nuage sombre, des poussières sont fortement chauffées par une étoile enfouie très brillante, formant la nébuleuse NGC 2023 (tache blanche au centre du cadre). Le rayonnement émis par une étoile brillante qui apparaît pas dans le champ représenté ici (cette étoile, Sigma de la constellation d'Orion se trouve au-dessus) dissocie le gaz interstellaire et perturbe les poussières le long du bord supérieur du nuage sombre. La nébuleuse dite Tête de cheval, dont on voit la forme caractéristique sur l'image en lumière visible, est une accumulation de matière située au bord du nuage. Sur l'image infrarouge prise par *ISO*, le nuage sombre est maintenant brillant : les poussières absorbent le rayonnement ultraviolet des étoiles et réémettent un rayonnement infrarouge. La nébuleuse de la Tête de cheval n'est plus visible en extinction ; on ne voit que sa « crinière » (flèche), due à l'émission des poussières fortement illuminées par l'étoile Sigma de la constellation d'Orion.

types de silicates interstellaires étaient essentiellement des olivines ou des pyroxènes (de formules chimiques respectives Fe_2SiO_4 et FeSiO_3 , l'atome de fer pouvant être remplacé par d'autres métaux comme le magnésium). De surcroît, l'élargissement des raies d'absorption caractérisait la présence de silicates amorphes, c'est-à-

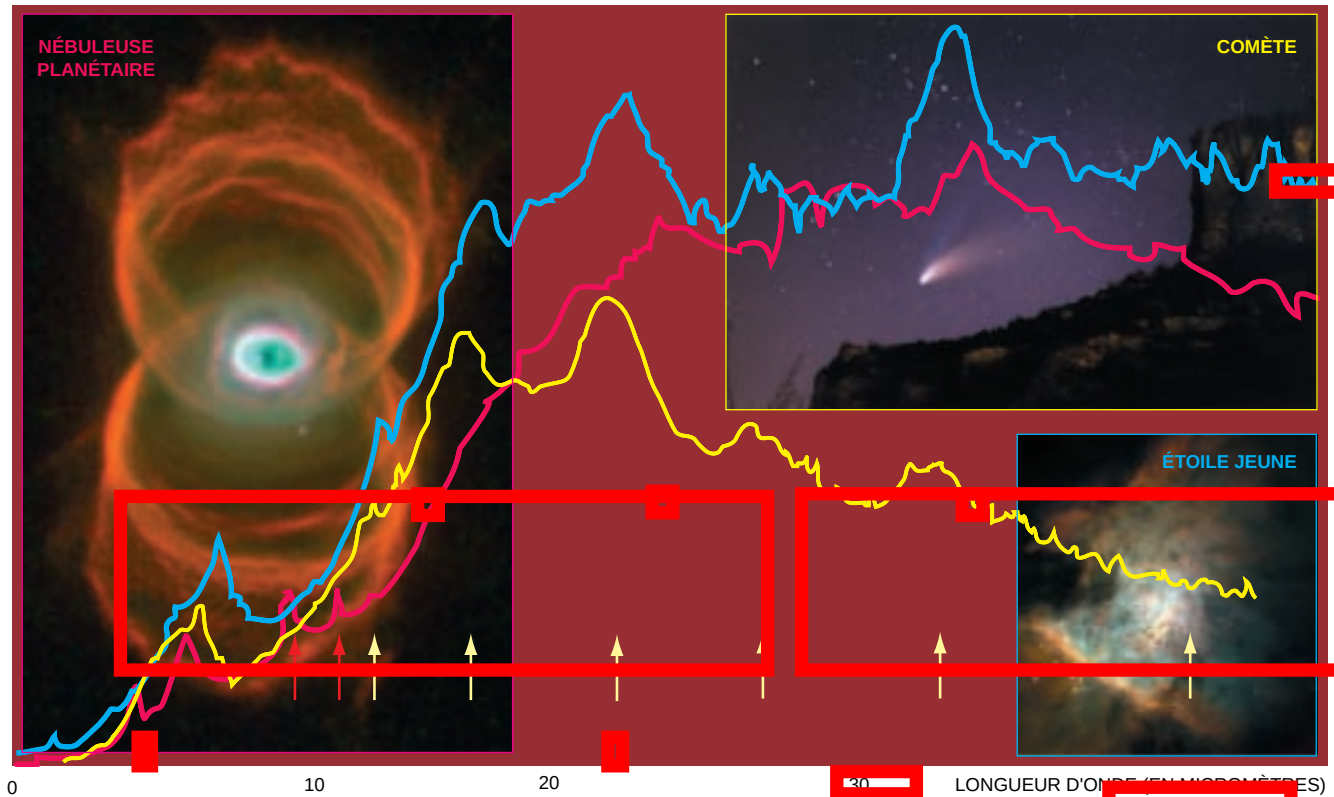
disposées régulièrement.

L'origine des silicates interstellaires

Le satellite *ISO* a montré que les disques de poussières présents autour d'étoiles jeunes émettent un rayonnement dont le spectre contient un

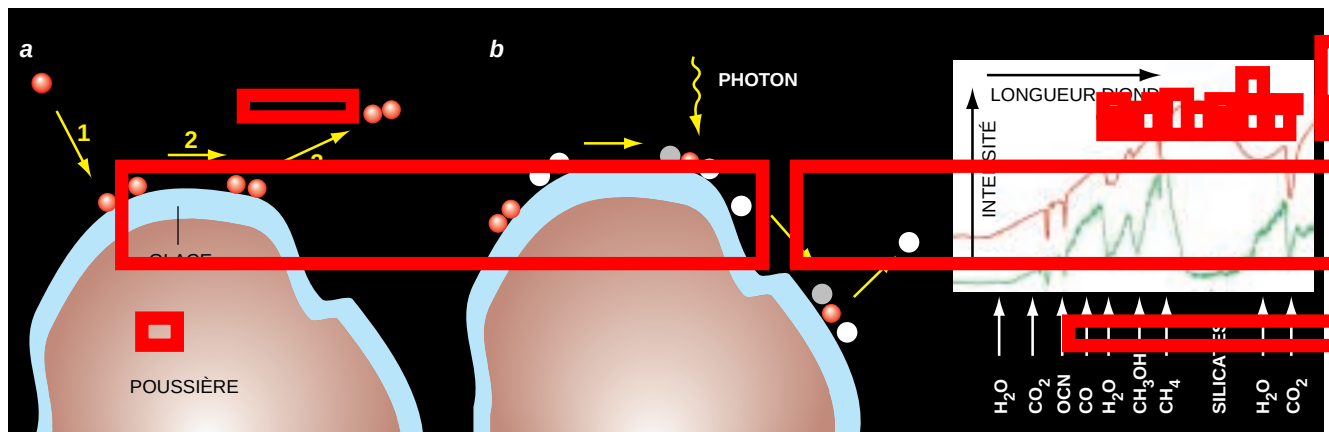
bué à des silicates cristallins, et non amorphes (voir la figure 2). De surcroît, ces spectres sont très proches de celui de la comète Hale-Bopp.

Une partie des poussières autour des jeunes étoiles est-elle d'origine cométaire? On sait que les étoiles se forment à partir de la matière interstellaire, c'est-à-dire de silicates que



2. LES SPECTRES DE RAYONNEMENT INFRAROUGE enregistrés par le satellite *ISO* permettent l'étude des poussières interstellaires. On sait depuis longtemps que ces poussières contiennent des silicates (des composés contenant des oxydes métalliques et de la silice) amorphes, c'est-à-dire dont les molécules ne sont pas ordonnées. Pourtant le satellite *ISO* a détecté, dans des nébuleuses planétaires

et autour des étoiles jeunes, des silicates cristallins (pics repérés par des flèches jaunes). Le spectre *ISO* de la comète de Hale-Bopp présente les mêmes pics. Dans les spectres des nébuleuses planétaires, on observe en outre des pics (flèches rouges) qui sont dus à des molécules aromatiques (composées de carbone et d'hydrogène, dans une configuration analogue à celle du benzène).



3. PRINCIPE DE FORMATION des molécules interstellaires à la surface des grains de poussière. À la surface des grains, des atomes sont piégés et peuvent former des molécules qui sont libérées dans le milieu interstellaire (a). Des photons peuvent aussi déclencher des

réactions chimiques (b). Le spectre enregistré par le satellite *ISO* (à droite, en vert) présente des raies d'absorption ; en le comparant au spectre réalisé en laboratoire (en rouge), on identifie différentes molécules présentes dans les glaces interstellaires.

l'on croyait être amorphes. Or la transformation de ces silicates amorphes en silicates cristallins nécessiterait une température de l'ordre du millier de kelvins, bien supérieure à la température des comètes ! À quelles étapes de la formation stellaire les silicates interstellaires passent-ils de l'état amorphe à cristallin ?

Le satellite *ISO* a également observé des silicates cristallins dans des nébuleuses planétaires, c'est-à-dire autour d'étoiles en fin de vie, lorsque celles-ci éjectent massivement leur matière dans le milieu interstellaire. Comment le milieu interstellaire contiendrait-il des silicates amorphes si les étoiles rejettent des silicates cristallins ?

Les silicates interstellaires sont-ils réellement amorphes ? Les chocs entre les poussières interstellaires ou l'irradiation des poussières provoqueraient-ils l'amorphisation de la surface extérieure, alors que le cœur serait cristallin ? La question reste ouverte, mais ce dernier scénario est invoqué par analogie avec ce qui se passe sur la Lune : dans notre Système solaire, les silicates sont observés sous forme cristalline, l'exception faite de certains minéraux observés sur la Lune et dont la surface devient amorphe sous le bombardement du vent solaire. À l'Université d'Orsay, ces expériences détermineront prochainement dans quelle mesure ce processus peut avoir lieu dans le milieu interstellaire.

Les petits grains interstellaires

Quand la matière interstellaire absorbe les rayonnements des étoiles, elle est chauffée et réémet des rayonnements qui dépendent de sa température, de la même façon qu'un filament d'ampoule change de couleur quand il est chauffé. La correspondance entre les longueurs d'onde du spectre infrarouge du milieu interstellaire et la taille des particules indique, nous le verrons, que les poussières interstellaires ont des dimensions comprises entre la taille d'une molécule et quelques dixièmes de micromètre pour les grains les plus gros.

Ces derniers reçoivent continûment de la lumière émise par des étoiles (on parle de « champ de rayonnement interstellaire »). Un équilibre s'établit entre l'absorption et l'émission de rayonnement, à une température comprise entre

10 et 100 kelvins (entre -263 et -173 °C). Le rayonnement émis est dans l'infrarouge lointain (à une longueur d'onde voisine de 100 micromètres).

Toutefois le spectre d'émission du milieu interstellaire dans l'infrarouge proche mesuré par le satellite *IRAS*, par des instruments au sol ou embar-

qués sur des ballons, montre plusieurs bandes d'émission à des longueurs d'onde voisines de 3,3, de 6,2, de 7,7, de 8,6 et de 11,3 micromètres ; découvertes au début des années 1970, ces bandes n'ont été expliquées de manière



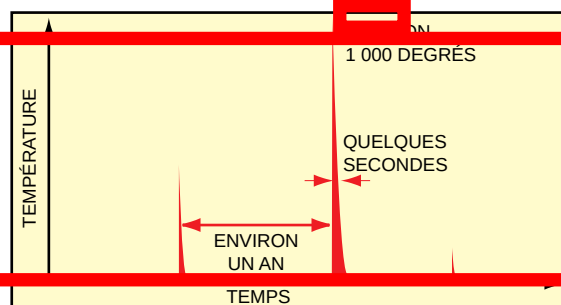
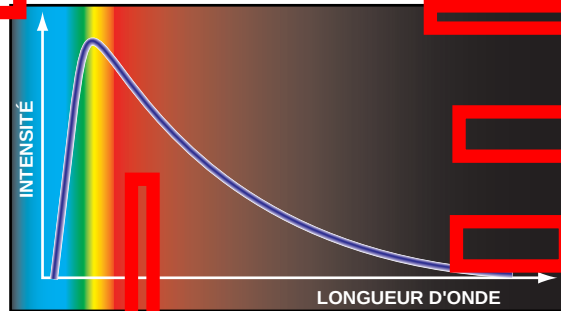
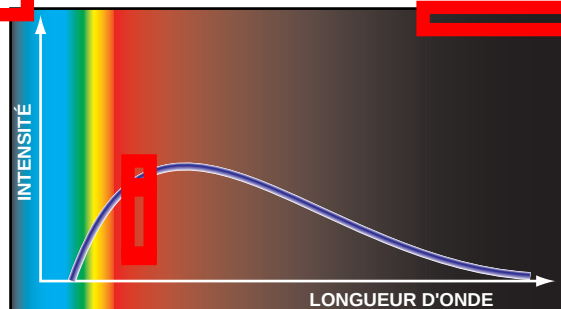
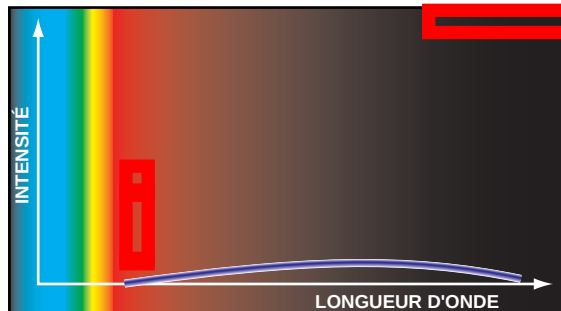
TEMPÉRATURE AMBIANTE



QUELQUES CENTAINES DE DEGRÉS



QUELQUES MILLIERS DE DEGRÉS



4. LES CORPS ÉMETTENT UN RAYONNEMENT qui dépend de leur température. Ce phénomène se observe quand on chauffe le filament d'une ampoule à incandescence : de noir, le filament tourne au rouge, puis au blanc. Progressivement son spectre se décale vers les courtes longueurs d'onde et le rayonnement devient visible. Un objet dont la surface est à la température ambiante émet surtout des infrarouges ; un objet chauffé à plusieurs milliers de degrés (tels le Soleil ou le filament d'une ampoule) émet de la lumière visible. Les plus gros grains interstellaires, très froids, émettent dans l'infrarouge lointain ; ils sont à l'équilibre thermique. En revanche, les grains les plus petits sont chauffés très rapidement chaque fois qu'ils absorbent un photon ultraviolet ou visible. Ils sont alors portés à une très haute température et se refroidissent très vite (*courbe inférieure*).

satisfaisante que dix ans après : elles résulteraient de l'émission infrarouge de grains très petits, constituants majeurs de la matière interstellaire.

Ces grains sont si petits

(leur diamètre est inférieur à une dizaine de nanomètres, ou milliardièmes de mètre) que l'énergie d'un seul photon ultraviolet ou visible suffit à les chauffer à une température de l'ordre de 1 000 degrés. Or, les plus petits grains reçoivent très peu de photons, parfois moins d'un par an. Après absorption d'un photon, un grain se refroidit en quelques secondes en émettant des rayonnements infrarouges. Entre l'absorption

de deux photons, le grain retombe à une température très basse (quelques kelvins). Un très petit grain émet donc l'essentiel de son énergie dans le peu de temps où il est très chaud (parfois pas plus de quelques secondes par an). Ce cycle est celui

du « chauffage impulsif » (voir la figure 4).

Quelle est la nature des grains de poussière qui émettent ces rayonnements ? En 1984, à l'Université Paris VI, Alain Léger et l'un d'entre nous (J.-L. Puget) ont remarqué que les bandes d'émission à 3,3, 6,2, 8,7, 8,6 et 11,3 micromètres ressemblaient à celles de grosses molécules d'hydrocarbures aromatiques, des molécules composées

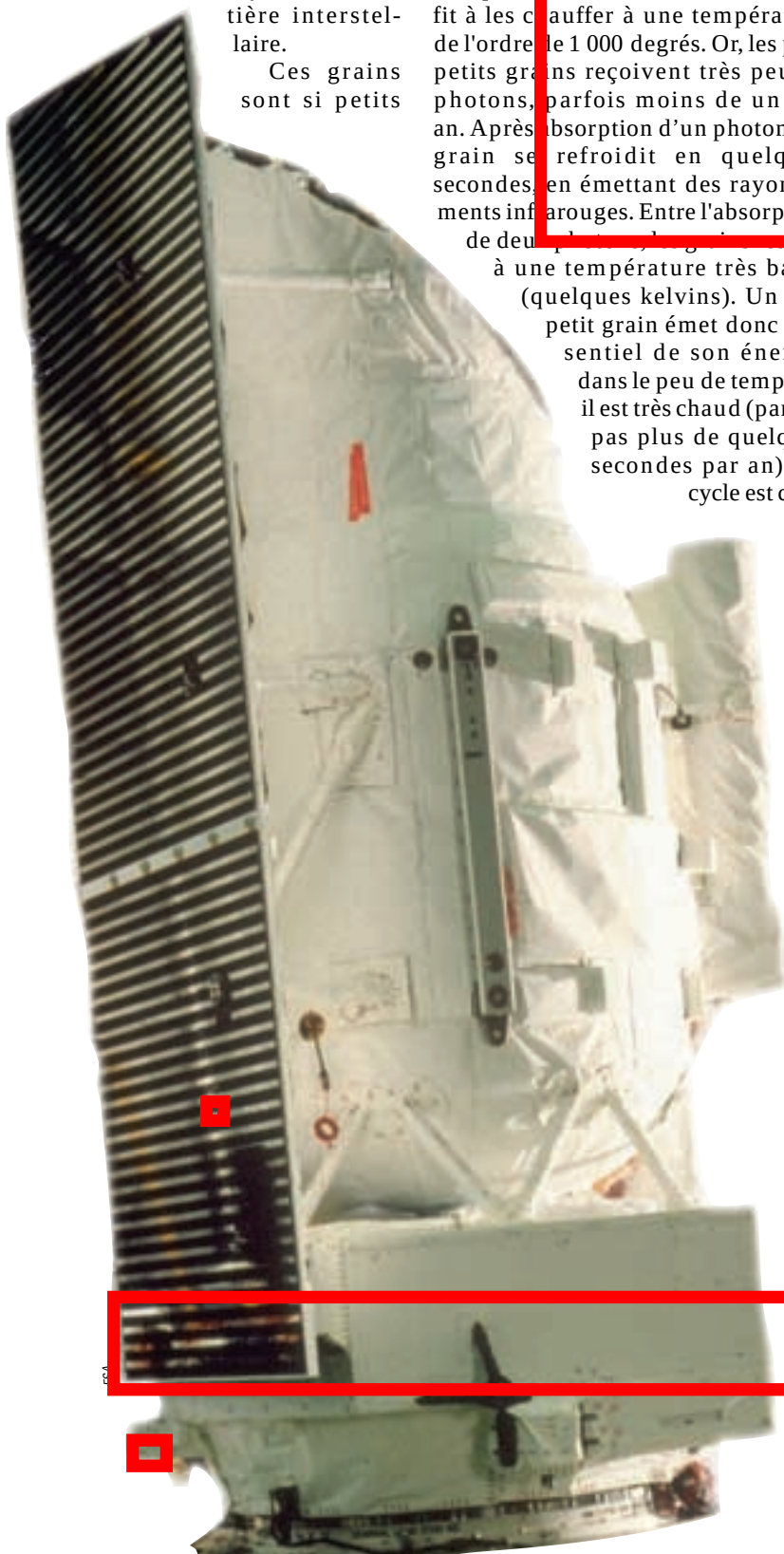
de cycles d'hydrogène, qui s'enchaînent pour former des cycles aromatiques tel celui du benzène C_6H_6). Les bandes d'émission du milieu interstellaire seraient dues à divers modes de vibration des liaisons entre deux atomes de carbone, ou entre un atome de carbone et un atome d'hydrogène de telles molécules.

La sensibilité des instruments d'ISO a révélé les bandes d'émission infrarouge quasiment partout dans notre Galaxie, ce qui confirme la présence des émetteurs de raies infrarouges à toutes les étapes du cycle interstellaire. Le fait que la forme du spectre observé par ISO soit inchangée alors que l'intensité du rayonnement varie typiquement de 1 à 10 000 est une éclatante confirmation du chauffage des poussières par le mécanisme impulsif.

Les observations et les modèles stellaires indiquent que les petits grains de poussière aromatiques sont rejetés par les étoiles riches en carbone à la fin de leur vie. Cependant les estimations montrent que ces étoiles ne sont probablement pas seules à produire les grains observés dans le milieu interstellaire. L'origine des hydrocarbures aromatiques du milieu interstellaire reste ainsi une question ouverte.

Leur structure aussi, car les spectres interstellaires sont comparés à des spectres enregistrés en laboratoire. Or les composés étudiés en laboratoire sont obtenus dans des conditions physiques qui ne sont pas identiques à celles du milieu interstellaire, et les conditions de formation sont

différentes (température, pression, densité de particules...). On ne sait notamment pas isoler et étudier, dans des conditions proches de celles du milieu interstellaire, des grosses molécules aromatiques hydrogénées, composées de plus de cinq cycles benzéniques, alors que l'intensité des bandes d'émission observées dans le



5. LE SATELLITE ISO a été lancé en 1995 par l'Agence spatiale européenne. Il mesure 5,3 mètres de haut et pèse 2,4 tonnes. Il a fonctionné pendant 29 mois, mesurant les rayonnements infrarouges de l'Univers. ISO a étudié la nature des poussières du milieu interstellaire et précisé le rythme de formation des étoiles au cours de l'évolution de l'Univers.

ciel par ISO caractérise des molécules contenant au moins une dizaine, voire une centaine de cycles.

Les glaces moléculaires

Des centaines de molécules ont été identifiées dans le milieu interstellaire, mais comment des molécules complexes se forment-elles dans l'espace? Même dans les régions les plus froides, le gaz interstellaire est très dilué (un dix millions de molécules par litre), et les collisions entre atomes ou entre molécules sont rares. Toutefois, les molécules complexes se forment nécessairement par réaction d'atomes ou de molécules simples, qui doivent donc se trouver côte à côte à un certain moment.

Le mystère a été résolu quand on a observé que, dans les nuages moléculaires denses, les poussières sont parfois à des températures très faibles (de l'ordre de dix kelvins), de sorte qu'un atome ou une molécule qui se colle à un grain (de rayon inférieur à un micromètre) restent collés à celui-ci, en raison de forces très faibles, nommées forces de Van der Waals (voir la figure 3).

Ainsi, les poussières se recouvrent progressivement d'un manteau de molécules formant des «glaces interstellaires». Ces glaces sont formées non seulement d'eau solide, mais aussi de monoxyde et de dioxyde de carbone (CO et CO₂), de méthanol (CH₃OH), etc. sous la forme solide.

Des nuages d'hydrogène qui se propagent à grande vitesse dans le milieu interstellaire, ainsi que des photons provenant des étoiles, irradient ces grains et leur apportent un coup d'énergie. Les molécules étant à proximité les unes des autres, l'énergie apportée aux atomes ou aux molécules des grains leur permet des associations chimiques et la formation de nouvelles molécules. Parfois les nouvelles espèces formées sont libérées dans le gaz : l'échange est permanent entre les molécules collées sur

les surfaces et les molécules présentes dans le gaz.

Le satellite ISO a identifié les molécules qui constituent les manteaux de glaces. Les vibrations et rotations des molécules correspondent à des absorptions ou à des émissions dans le spectre infrarouge, à des longueurs d'onde caractéristiques de ces molécules (voir la figure 3). Les étoiles du nuage de poussières se sont formées et qui rejette ainsi toutes les molécules dans la phase gazeuse. Ces molécules voyagent dans notre Galaxie et participent à nouveau à la formation de nuages interstellaires,

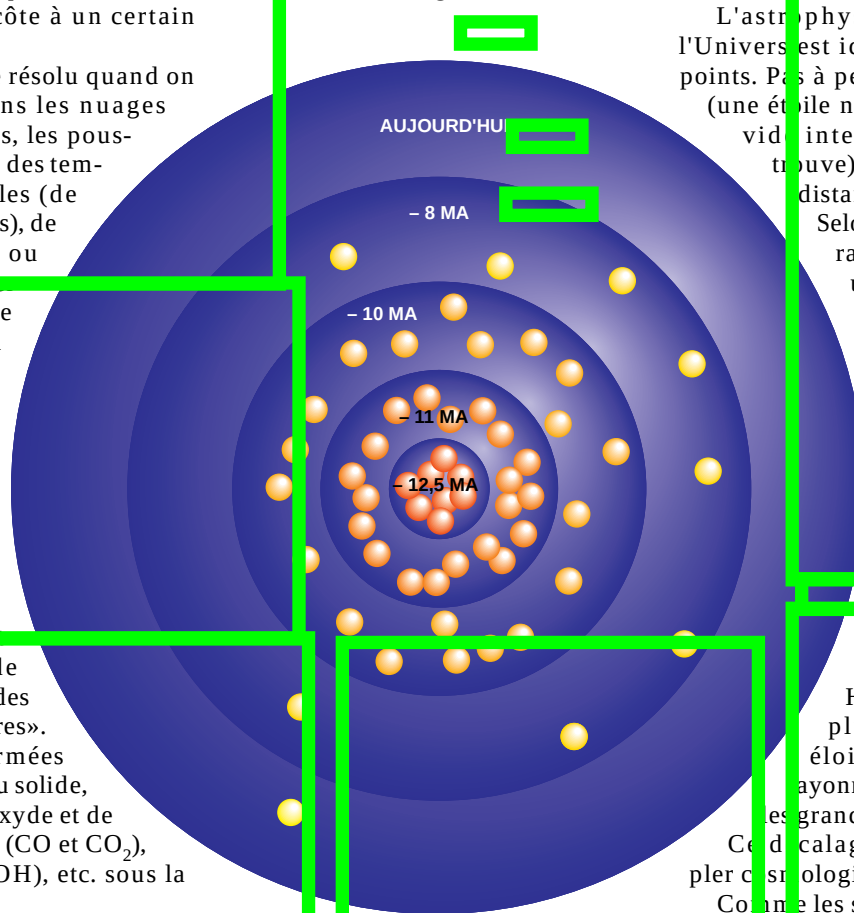
et ainsi de suite. Ce cycle de matière est à l'origine de l'enrichissement moléculaire de notre Galaxie au cours du temps.

Les observations cosmologiques

ont révélé la nature de la matière interstellaire dans le voisinage du Système solaire et donné des informations sur l'Univers dans son ensemble. Parmi les grandes questions de la cosmologie contemporaine figure celle de la formation des galaxies et, plus généralement, celle de l'histoire de la formation des étoiles.

L'astrophysique suppose que l'Univers est identique en tous ses points. Pas à petite échelle, bien sûr (une étoile n'est pas identique au vide interstellaire où elle se trouve), mais à l'échelle des distances intergalactiques.

Selon cette hypothèse, les rayonnements émis par un élément chimique, tel l'hydrogène, devraient toujours être à la même longueur d'onde. Pourquoi, alors, les galaxies qui nous envoient des rayonnements qui semblent déca-



6. LE SATELLITE ISO A OBSERVÉ DES GALAXIES qui contribuent au fond diffus extragalactique. Ce fond provient de l'émission cumulée de toutes les galaxies depuis les premiers instants de l'Univers. Comme la lumière se propage à vitesse finie, plus les galaxies sont éloignées, plus on les voit dans le passé. Leurs émissions sont de plus en plus décalées vers les grandes longueurs d'onde. De ces émissions, on a déduit que pour une étoile de type Soleil formée aujourd'hui, il s'en formait 8 il y a 8 milliards d'années, 20 il y a 10 milliards d'années, 10 il y a 11,5 milliards d'années, 4 il y a 12 milliards d'années (sur cette figure, les échelles de taille de l'Univers ne sont pas respectées).

En 1929, l'astronome américain Edwin Hubble montra que plus les galaxies sont éloignées, plus leur rayonnement est décalé vers les grandes longueurs d'onde. Ce décalage est un effet Doppler cosmologique.

Comme les sources décalées vers le rouge sont plus éloignées de la Terre et comme la lumière se propage à la vitesse de 300 000 kilomètres par seconde, le rayonnement qui est le plus décalé a voyagé pendant de grandes distances et a donc mis beaucoup de temps à nous parvenir : en regardant aux grands décalages vers le rouge, les astronomes explorent le passé de l'Univers.

La galaxie la plus lointaine jamais détectée se trouve à un décalage vers le rouge de l'ordre de 6,7, ce qui correspond à un Univers ayant dix pour

cent de son âge actuel (estimé à 12,6 milliards d'années). Aujourd'hui, les astrophysiciens mesurent systématiquement le décalage vers le rouge de toutes les galaxies détectées dans certaines régions du ciel, afin de comprendre

comment se sont formées les galaxies, et comment elles ont évolué vers les galaxies qui nous entourent.

À l'Observatoire franco-canadien d'Hawaii, notamment, une équipe utilise le télescope installé sur le volcan Mauna Kea pour étudier le décalage vers le rouge des galaxies

dans cinq champs qui mesurent chacun quelques minutes d'angle de côté. C'est ainsi qu'est apparue une augmentation considérable (un facteur dix environ) de la fréquence de formation d'étoiles entre l'époque actuelle et il y a cinq milliards d'années.

Ce résultat a été confirmé et étendu à l'aide du Télescope spatial *Hubble*, qui a accumulé, sur un même champ du ciel, des centaines d'heures d'observation, fournissant l'image la plus profonde jamais obtenue en astronomie optique. Ces observations semblaient également indiquer un maximum d'activité de formation d'étoiles il y a cinq milliards d'années.

Toutefois, pour notre Galaxie, la découverte des poussières, évoquée précédemment, a montré qu'une grande partie de la lumière émise par les

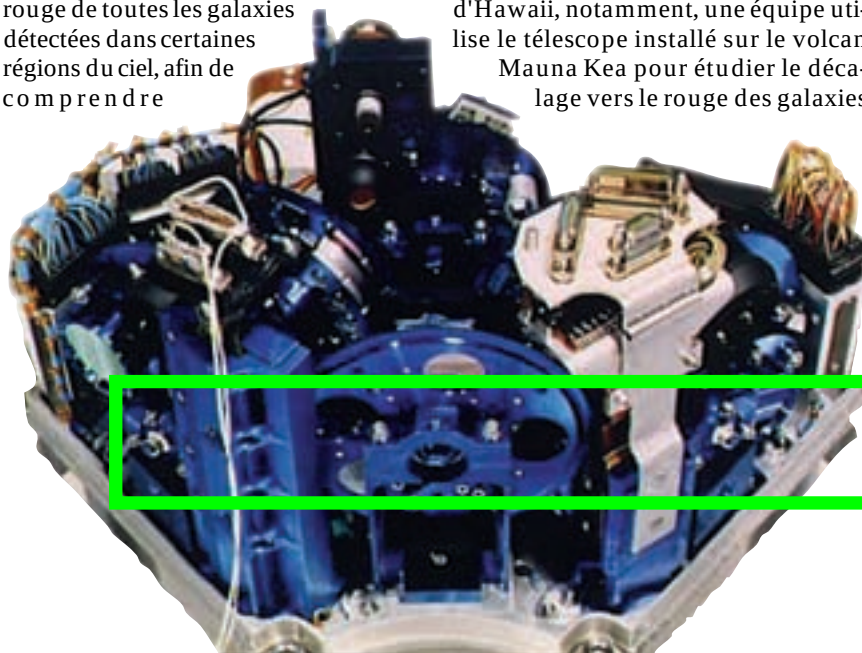
étoiles est absorbée. Qu'en est-il pour les galaxies lointaines? Cette question est restée controversée. L'écran de poussières est-il homogène, c'est-à-dire les poussières sont-elles réparties de façon diffuse, cachant de la même façon tous les objets distants? Ou bien les poussières sont-elles confinées à l'intérieur même des galaxies?

Il y a un peu plus de dix ans, le satellite *IRAS* corrobora la seconde hypothèse. Les « galaxies infrarouges » : ces galaxies forment beaucoup plus d'étoiles que notre Galaxie, par exemple, et elles émettent jusqu'à 95 pour cent de leur énergie dans le domaine infrarouge. Manifestement le recensement des étoiles dans l'Univers était biaisé quand les astronomes n'étudiaient que les rayonnements optiques.

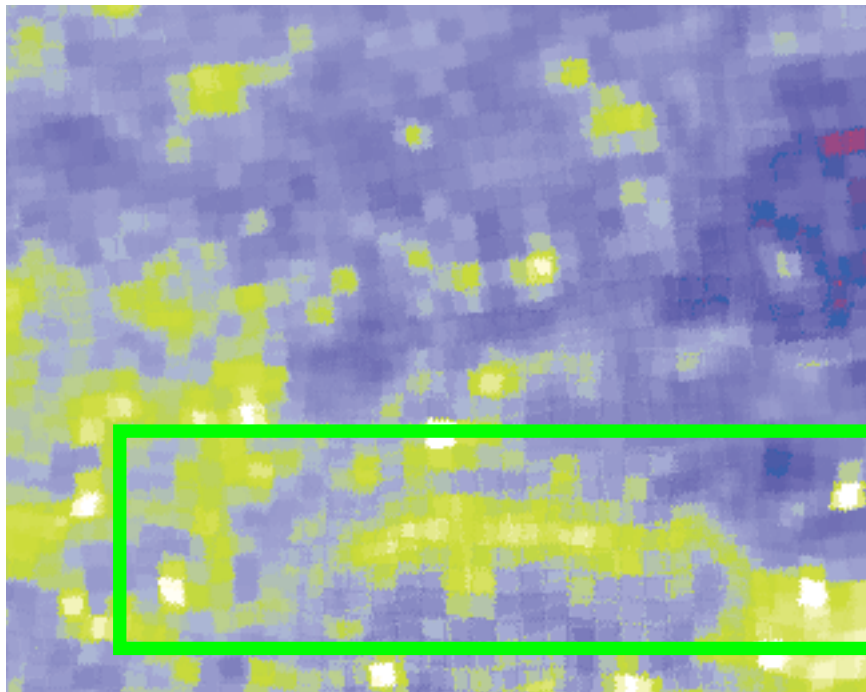
On sait aujourd'hui que, lors des collisions entre les galaxies, la formation d'étoiles peut être centuplée, mais invisible, en raison des considérables concentrations de gaz et de poussières, qui absorbent le rayonnement. Ce sont de telles collisions qui engendrent les galaxies infrarouges découvertes par *IRAS*.

Ces épisodes ne sont-ils que de spectaculaires événements, trop rares pour influencer leur évolution? Ou

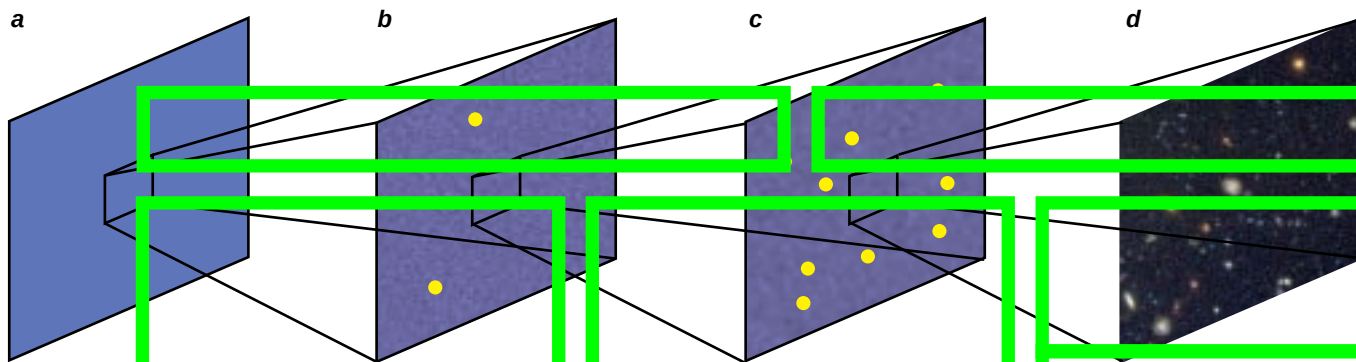
au contraire, les collisions de galaxies, fréquentes dans le passé, ont-elles joué un rôle majeur dans leur évolution? Dans cette dernière hypothèse, une bonne partie de l'histoire de la formation d'étoiles dans l'Univers ne serait observable que dans le domaine infrarouge.



7. LA CAMÉRA ISO-CAM embarquée sur le satellite *ISO* a été fabriquée sous la responsabilité de Catherine Césarsky et de ses collègues du CEA, et testée à l'Université d'Orsay. Cette caméra enregistre les rayonnements infrarouges à des longueurs d'onde comprises entre 2 et 16 micromètres. Le champ angulaire de la caméra était remarquablement petit : quelques secondes d'arc seulement, soit un cheveu vu à 20 mètres de distance.



8. CE CHAMP PROFOND a été observé par l'instrument *ISOPHOT* à une longueur d'onde de 175 micromètres. Cette carte ne représente qu'une très petite partie du ciel. Les filaments brillants (en vert) correspondent à de la matière présente dans notre Galaxie ; cette matière est située au premier plan. Se superposent ensuite des sources ponctuelles (points verts isolés ou blancs) qui, elles, sont extragalactiques. Ces sources sont des galaxies, parfois très jeunes (elles se sont formées quand l'Univers n'avait que trois milliards d'années, contre 13 aujourd'hui). En dehors des filaments brillants et des sources ponctuelles, on distingue un fond granuleux (en bleu), qui correspond à l'ensemble des sources extragalactiques non résolues.



9. LE FOND EXTRAGALACTIQUE apparaît uniforme à grande échelle (a), les autres galaxies formant un fond granuleux. La caméra **ISOCAM** mais il est dû à l'émission de galaxies non résolues (c). **ISOPHOT** permet de résoudre environ dix pour cent des galaxies (b), entre c et d).

Le satellite *ISO* a apporté des éléments de réponse qui vont dans le sens de la seconde hypothèse. Plusieurs perceptions du fond extragalactique ont été très longuement observées. En raison des performances exceptionnelles des détecteurs et du mode d'observation (*ISO* travaille en mode pointé, les détecteurs étant fixés sur la partie du ciel à analyser, tandis qu'*IRAS* fonctionnait en mode de balayage), *ISO* a découvert des objets bien moins lumineux, donc plus lointains, qu'*IRAS*.

La caméra *ISOCAM* a recherché les galaxies lointaines, donc très peu brillantes, à des longueurs d'onde égales à 6 et à 15 micromètres. Le gain en sensibilité par rapport à *IRAS* est spectaculaire : environ 3 000. Le relevé le plus profond avec *ISOCAM* a été effectué sur une partie du ciel qui a été surnommée « champ profond de Hubble » : c'est ce champ qui a été exploré par le Télescope spatial *Hubble* en lumière visible et dans le domaine ultraviolet. *ISO* a trouvé bien moins de sources que *Hubble*, mais il nous a appris que l'énergie totale rayonnée par les quelques sources infrarouges détectées est comparable à celle de toutes les sources détectées par *Hubble*.

Les sources détectées par *ISOCAM* ne sont donc pas du même type que celles observées par *Hubble*. Ce résultat spectaculaire pose des problèmes à l'ensemble des astronomes qui ont bâti depuis plus de 20 ans une compréhension du fond extragalactique à partir des observations du domaine ultraviolet et visible.

L'infrarouge lointain a été observé avec le photomètre *ISOPHOT* qui, malgré sa faible résolution spatiale, permet pour la première fois d'observer les galaxies lointaines à une longueur d'onde de 175 micromètres. À cette longueur d'onde, les sources détec-

tées sont bien moins nombreuses que dans l'ultraviolet, dans le visible ou dans l'infrarouge proche. Cependant, leur nombre est bien supérieur à celui que l'on obtient quand on extrapole l'émission des galaxies proches observées avec *IRAS*.

De ce fait, les galaxies détectées dans les relevés profonds cosmologiques ont une nature bien différente de celles qui ont été détectées avec *IRAS*. Ces galaxies sont plus lointaines (et donc plus jeunes), et elles ont des propriétés qui diffèrent considérablement des galaxies locales, plus proches. Cette découverte confirme l'hypothèse qui stipulait que le rythme de la formation d'étoiles fut jadis plus élevé qu'aujourd'hui.

Cette très forte évolution des galaxies distantes s'observe également quand on mesure une composante plus diffuse, provenant de l'émission intégrée des galaxies sur toute l'histoire de l'Univers, le fond extragalactique. Pour comprendre à quoi correspond ce fond, imaginons que nous soyons à bord d'un petit voilier qui passe le cap Horn : nous voyons parfaitement les mouvements des vagues déchaînées. En revanche, si nous sommes en avion, l'océan n'est alors plus qu'une étendue bleue uniforme.

Ce fond d'apparence uniforme a été observé à des longueurs d'onde comprises entre 100 micromètres et 1 millimètre.

Le satellite *COBE*. La forte intensité de ce fond montre qu'une grande partie de la formation d'étoiles est cachée du domaine visible et observable seulement dans le domaine infrarouge : l'énergie émise par toutes les galaxies dans l'Univers est environ deux fois plus grande dans le domaine infrarouge que dans le domaine visible.

Les galaxies dont le rayonnement constitue ce fond émettent beaucoup plus d'énergie dans le domaine infrarouge que les galaxies proches de nous.

Ce phénomène est une autre signature du changement profond des propriétés des galaxies depuis leur formation jusqu'à aujourd'hui. Il conduit à proposer que le rythme de formation d'étoiles fut constant il y a 10 à 12 milliards d'années, mais 20 fois plus fort qu'aujourd'hui (en supposant une durée de vie de 10 milliards d'années). Avec *ISOPHOT*, à une longueur d'onde de 175 micromètres, les galaxies détectées ne représentent que dix pour cent du fond. En revanche, à la longueur d'onde de 15 micromètres, le fond extragalactique est presque totalement résolu en sources individuelles.

Seule une petite partie de l'Univers est visible aujourd'hui, grâce au satellite *ISO*, mais cette partie permet pour la première fois de mieux étudier l'évolution des galaxies depuis la formation de l'Univers.

Alain ABERGEL, François BOULANGER, Guilaine LAGACHE, Emmanuel DARTOIS et Jean-Loup PUGET travaillent à l'Institut d'Astrophysique Spatiale de Orsay.

F. COMBES, P. BOISSIE, A. MAZURE, A. BLANCHARD, *Galaxies et cosmologie*, Interéditions / Éditions du CNRS, 1991.

D. ALLOIN, *Les galaxies*, Éditions Flammarion (collection Dominos), 1998.

The Universe as seen by ISO, sous la direction de P. Cox et M. Kessler, *ESA Proceedings*, SP-427, 1999.

Le gravidyne

ROLAND LEHOUCQ

Ne pouvons échapper à l'attraction terrestre à l'aide d'un vaisseau-haltère dont la longueur varie à des instants précis de sa trajectoire.

Cyrano de Bergerac a retardé le duc de Guiche en décrivant sept moyens farfelus d'aller sur la Lune ; Émile de Cyrano, le physicien russe V. Béletski a proposé un engin spatial qui paraît étrange au premier abord, mais dont le principe est uniquement fondé sur une conséquence des lois de la gravitation. Dans le champ gravitationnel d'une planète, l'attraction exercée sur un solide étendu diffère de celle exercée sur un point matériel de même masse ; en variant la forme d'un solide, on modifie l'intensité de la force d'attraction qu'il subit et l'on peut le lancer vers les étoiles.

Comment expliquer cette variation ? Quand l'attraction gravitationnelle est uniforme, la force d'attraction est identique en tous les points de l'objet : l'attraction qu'elle s'exerce sur un objet étendu est égale à la force qui s'exerce sur une masse équivalente placée au centre de gravité de l'objet. En revanche, les parties d'un corps étendu plongé dans le champ gravitationnel d'une planète, dans un champ dont l'intensité décroît avec le carré de la distance entre le corps et la planète, subissent des attractions qui peuvent être fort inégales. Chaque partie du corps d'un satellite par exemple, tombe alors vers la planète avec une accélération différente.

Dans le champ terrestre, cet effet est sensible lorsque la dimension du satellite dépasse plusieurs dizaines de kilomètres.

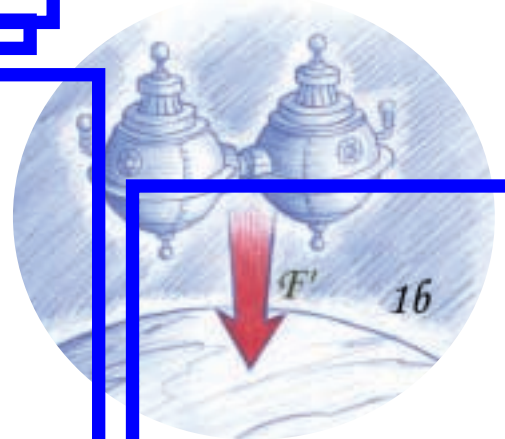
Les parties lointaines étant moins attirées que les parties proches, le satellite est étiré le long de l'axe qui le lie son centre à celui de la planète. Les marées témoignent de cet étirement : sur Terre, les océans sont déformés par l'attraction de la Lune.

ATTRACTION SUR UN GRAND SATELLITE

L'engin que nous nous proposons d'utiliser pour nous déplacer dans le cosmos est en forme d'haltère : deux sphères identiques reliées par une barre rigide de masse négligeable par rapport à celle des sphères. Nous supposons, de surcroît, que l'axe de la barre est perpendiculaire au plan de l'orbite. Les sphères subissent des attractions terrestres de même intensité, car elles sont situées à la même distance du centre de la Terre, et de directions légèrement différentes puisque les droites qui joignent leur centre à celui de la Terre forment un petit angle.

La force d'attraction résultante F , orientée vers le centre de la Terre, est presque égale en intensité à la force F' que subirait un point matériel de même masse que notre haltère et situé en son centre de gravité. Presque, mais pas tout à fait ! La force F est en fait inférieure à la force F' (voir les figures 1a et 1b) : l'écart relatif entre les deux forces est proportionnel au carré du rapport entre la longueur de l'haltère et la distance au centre de la Terre (tant que la longueur de l'haltère reste petite devant la distance de son centre de gravité au centre de la Terre). Dans le cas limite où les sphères seraient écartées d'une distance énorme, la force exercée serait presque nulle, puisque cette dernière décroît avec le carré de la distance, alors que la force exercée sur la même masse placée au centre de gravité de l'ensemble ne l'est pas.

En pratique, à moins que le satellite ne soit très grand, l'écart entre les

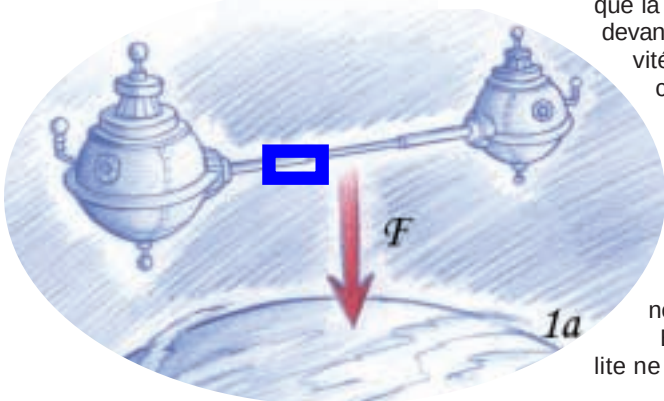


deux forces est faible. Ainsi, pour la station spatiale *Mir*, dont la taille est de 30 mètres et la distance au centre de la Terre d'environ 6 800 000 mètres, l'écart relatif des deux forces, $(F' - F)/F$, vaut trois cent milliardièmes (3×10^{-13}). En d'autres termes, un corps très allongé subit une attraction inférieure à celle d'un corps ramassé sur lui-même. Presque insensible sur de petits satellites, cette différence est ici mise à profit pour concevoir un procédé original de déplacement spatial.

UN VAISSEAU SPATIAL PULSANT

La modification de l'orbite est la clé du voyage spatial. Pour qu'un satellite quitte le voisinage terrestre à partir d'une orbite elliptique, il faut dépenser de l'énergie, c'est-à-dire augmenter l'excentricité e (l'allongement de l'ellipse) de l'orbite initiale jusqu'à ce qu'elle dépasse l'unité, valeur au-delà de laquelle la trajectoire devient hyperbolique (voir la figure 2).

Sans apport d'énergie, l'excentricité de l'orbite est constante. Le mouvement d'un solide est en général compliqué par l'interaction entre le déplacement du centre de gravité du solide et la rotation autour de son centre de gravité. Pour des raisons de symétrie, un solide comme notre haltère placé initialement avec son axe de symétrie perpendiculaire au plan de son



Dessins de Bruno Vacaro

orbite garde cette orientation. L'excentricité de la trajectoire dépend alors du temps et oscille périodiquement entre deux valeurs extrêmes : minimale au périhélie (le point de l'orbite le plus proche de la Terre) et maximale à l'apohélie (le point le plus éloigné de la Terre). Ces oscillations sont de très faibles amplitudes, et l'orbite de l'haltère est très proche de l'orbite elliptique d'un point matériel de même masse.

Imaginons maintenant que notre vaisseau-haltère pulse, c'est-à-dire qu'il se contracte et se déploie rapidement sur toute sa longueur à des instants bien choisis. Partant du périhélie, l'haltère parcourt une demi-révolution jusqu'à son apohélie, où l'excentricité atteint sa valeur maximale. A cet instant, l'haltère se replie : sa longueur devient très faible, et le vaisseau se déplace alors comme un point matériel, c'est-à-dire en suivant un arc d'ellipse dont l'excentricité est celle atteinte à l'apohélie.

Revenant au périhélie, en un point plus proche de la Terre que le périhélie précédent, l'haltère se déploie à nouveau. L'excentricité de sa trajectoire augmente et lorsque le vaisseau arrive à un nouvel apohélie, plus éloigné de la Terre, la trajectoire atteint une excentricité supérieure à celle atteinte lors du précédent passage. L'haltère se replie alors pour conserver la nouvelle valeur de l'excentricité jusqu'à l'instant où il pourra se déployer à nouveau.

TRANSFERT D'ÉNERGIE ET RÉSONANCES

Après de nombreuses pulsations, l'excentricité de l'orbite aura varié notablement et, lorsqu'elle dépasse l'unité, le vaisseau échappe définitivement à l'attraction terrestre. La trajectoire suivie est une spirale dont le nombre de spires est égal au nombre de pulsations de l'haltère (voir la figure 3). Ce vaisseau spatial est dénommé gravityne.

D'où provient l'énergie gagnée par le gravityne ? En changeant de forme, le gravityne fait varier l'intensité de la force d'attraction qu'il subit, c'est-à-dire qu'il modifie son énergie potentielle gravitationnelle. Celle-ci augmente lorsqu'il se déploie et diminue lorsqu'il se contracte (sa valeur est négative). Cependant, n'oublions pas que ces variations ne se produisent pas à la même distance de la Terre : le déploiement s'effectue à l'apohélie, et la contraction au périhélie. Ainsi l'énergie du gravityne augmente plus qu'elle ne diminue.

Cette énergie provient du mécanisme qui modifie la géométrie du gravityne. Puisque la force gravitationnelle est attractive, les deux sphères de l'haltère sont attirées vers le centre de la Terre ; elles ont alors tendance à se rapprocher. Nous récupérons donc de l'énergie lors de la contraction du gravityne, alors que nous en dépensons pour le déployer. La différence est égale au gain d'énergie orbitale : l'énergie dépensée pour faire pulser le gravityne est transformée en énergie orbitale.

Le pilotage du gravityne est aussi fondé sur l'utilisation judicieuse des résonances. La période de pulsation du gravityne coïncide exactement avec la période de révolution orbitale. On augmente l'énergie du gravityne en variant sa longueur à des moments bien choisis, tout comme un enfant accélère le mouvement de sa balançoire en dépla-

çant son corps aux bons moments, ou comme le tireurs du grand encensoir de Saint-Jacques-de-Compostelle augmentent l'amplitude des oscillations en modifiant périodiquement la longueur de la corde de suspension.

UNE SOLUTION MIRACLE ?

Ce mécanisme d'amplification paramétrique serait donc parfait si le calcul ne nous ramenait à la dure réalité. À chaque cycle, l'excentricité du gravityne augmente d'une quantité proportionnelle à $(l/a)^2$, où l est la distance des deux masses et où a est la longueur du demi grand axe de l'orbite (tant que l/a est assez petit).

Pour atteindre une excentricité unité, synonyme d'échappement, il faudra environ $(a/l)^2$ cycles. Si l'orbite de départ d'un gravityne d'un kilomètre de longueur a un demi grand axe de 7 000 kilomètres, il lui faudra environ 49 millions de révolutions pour se libérer, ce qui prendra 9 000 ans. Un gravityne de 100 kilomètres de longueur atteindrait cet objectif en moins d'un an.

Ce procédé de navigation interplanétaire permet aussi d'imaginer une possibilité inédite de sauvetage d'un cosmonaute perdu hors de sa base spatiale et sans moyen de propulsion : par des pulsations adéquates obtenues en nageant la brasse, il modifiera son orbite et pourra rejoindre son vaisseau. Mais surtout ne demandez pas combien de temps il mettra...

Roland LEHOUCQ est astrophysicien au Service d'astrophysique du CEA.

V. BÉLETSKI, *Essai sur le mouvement des corps cosmiques*, Éditions Mir, 1986.

A. CAZENAVE et **A. BRAHIC**, *L'effet des marées dans le Système solaire*, in Dossier Les terres célestes, *Pour la Science*, avril 1999.

J. S. LOSADA, *La physique de l'encensoir*, in *Pour la Science*, septembre 1990.





Premiers jumeaux : frères ennemis?

JEAN-PAUL DELAHAYE

En conditionnant les inverses des nombres premiers jumeaux, un mathématicien obstiné découvre des erreurs dans les microprocesseurs.

Il arrive que l'écart entre deux nombres premiers consécutifs soit 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, etc. Le problème, comme nous le verrons, est dans le etc.!

Ces paires sont dénommées des nombres premiers jumeaux ; si l'on ne sait pas très bien qui s'y intéresse le premier, elles sont l'objet d'une grande attention depuis un siècle. Leur étude a donné lieu à de nombreuses spéculations mathématiques et à de non moins nombreux

calculs informatiques. L'un d'eux, dont les calculs ont été effectués sur un ordinateur, a mené un paisible mathématicien à faire trembler sur sa base la puissante industrie des microprocesseurs ; d'autres ont amené la découverte de nouvelles propriétés des nombres premiers. Ainsi, par certains côtés, l'arithmétique ressemble plus à une discipline expérimentale,

proche de la physique, qu'à une branche des mathématiques dites «pures».

EN TROUVE-T-ON TOUJOURS ?

Existe-t-il une infinité de nombres premiers jumeaux ? C'est l'une des plus célèbres conjectures mathématiques : on ne sait ni prouver qu'il n'y a qu'un nombre fini de nombres premiers jumeaux ni démontrer le contraire. La situation est choquante, car moins de 30 mots suffisent pour démontrer qu'il existe une infinité de nombres premiers : *S'il n'y en avait qu'un nombre fini, leur produit additionné de 1 serait divisible par l'un d'eux, donc 1 aussi, ce qui est absurde.* En même temps, tout semble s'opposer à ce que l'on sache (avec certitude) si, oui ou non, il existe une infinité de nombres premiers jumeaux. Les deux problèmes sont très proches, pourtant l'un est facile, alors que l'autre résiste obstinément.

Bien sûr, les calculs montrent que l'on trouve toujours des nombres premiers jumeaux, aussi loin qu'on aille. On a cherché aussi à compter le nombre précis de premiers jumeaux inférieurs à n . Ce calcul, par recherche exhaustive, a été mené jusqu'à la valeur de n égale à 10^{15} (un million de milliards) : pour 29 844 570 422 669 nombres premiers inférieurs à 10^{15} , on compte exactement 1 177 209 242 304 paires de nombres premiers jumeaux, soit environ quatre pour cent.

Les mathématiciens ont trouvé des nombres jumeaux beaucoup plus grands que cette valeur. Actuellement, la plus grande paire, découverte il y a quelques semaines, est composée de deux nombres de 11 755 chiffres chacun qui sont : 361700055.2^{39014} plus et moins 1. Ces nombres ont été capturés par Henri Lifchitz, un ingénieur français passionné des nombres premiers (en 1971, il avait déjà publié une table des nombres premiers inférieurs à 20 millions).

Les nombres premiers se raréfient ;

1. LE BUG DU PENTIUM : AVEC THOMAS NICELY, TESTEZ VOTRE MACHINE!

Le problème du *Pentium*, dévoilé par Thomas Nicely, a été décorqué, et des cas d'erreurs très simples ont été repérés. Le pire cas a été découvert par Tim Coe : $4195835.0 / 3145727.0$ donne 1.333739068902... au lieu de 1.333820449136... sur le *Pentium*. L'erreur est 10 000 fois supérieure à celle que donne une calculette à 50 francs : il ne s'agit pas d'une erreur normale d'arrondi.

Pour le petit programme de trois instructions : $B = 4.1 - 1.1$; $A = 699306 * B$; $Q = A / B$, le *Pentium* donne $Q = 699263.3$ au lieu de $Q = 699306$. Dans ce programme, il ne faut pas remplacer $4.1 - 1.1$ par 3, car le *Pentium* calcule en binaire et ni 4.1 ni 1.1 ne s'écrivent exactement en base 2.

Pour le quotient $4.9999999/14.999999$ le *Pentium* donne 0.33332922 au lieu de 0.33333329. Là non plus, il ne s'agit pas d'une erreur normale d'arrondi, mais d'une erreur dans la conception même de l'algorithme de division du processeur mathématique des premières versions du *Pentium*.

Une analyse détaillée montre que c'est souvent avec des nombres proches de l'unité que le *Pentium* se trompe. Or il se trouve que, dans toutes sortes de calculs, de tels nombres apparaissent naturellement, ce qui fait que, même si peu de divisions sont mal calculées, ce sont par malchance des divisions qu'on a la plus grande probabilité de rencontrer. Vaughan Pratt a ainsi montré que, si l'on s'intéresse aux quotients x/y , avec x et y variant entre 1 et 100 par pas de $1/100000$, la probabilité de tomber sur une erreur du *Pentium* est de $1/2000$, ce qui est très loin du $1/10 \times 10^9$ indiqué par Intel pour se défendre!

L'erreur du *Pentium* n'est pas bénigne! Remarquons cependant que les erreurs d'arrondi sont normales et inévitables, et qu'elles se produisent même avec des microprocesseurs sans bug. Leur accumulation doit être contrôlée : un rapport du *General Accounting Office* américain cite le cas d'un missile *Patriot* qui, pendant la guerre du Golfe, n'a pas intercepté sa cible, à la suite d'accumulations d'erreurs d'arrondi, causant la mort de 28 personnes.



Thomas Nicely

aux alentours de n , il y a environ $1/\log n$ nombres premiers (exemple : puisque $\log 1\,000\,000$ égale 13,81, vers le millionième nombre entier, il y a environ un nombre premier sur 14). Ce «théorème des nombres premiers» a été démontré en même temps par le Français Jacques Hadamard et le Belge Charles-Jean de la Vallée Poussin en 1896. (Ils vécurent respectivement jusqu'à l'âge de 98 et 96 ans : le meilleur moyen pour vivre âgé est de démontrer un tel théorème !)

PARÉFACTION

On constate que les nombres premiers jumeaux considérés parmi les nombres premiers se raréfient aussi. Un argument heuristique (c'est-à-dire qui «suggère» sans prouver rigoureusement) conduit à penser que les nombres premiers jumeaux ont une densité égale à $1/\log n$ parmi les nombres premiers (ou, ce qui revient au même, une densité de $1/(\log n)^2$ parmi les nombres entiers). L'argument est simple : «la probabilité que p et que $p+2$ soient simultanément premiers est le produit de la probabilité que p soit premier par celle que $p+2$ le soit, car les événements sont indépendants et «donc» le « $1/\log n$ » du théorème des nombres premiers fournit un « $1/(\log n)^2$ » car la probabilité de la conjonction de deux événements indépendants est le produit de leurs probabilités).

Cet argument est non seulement insuffisant, mais extrêmement dangereux. En l'appliquant à p et à $p+1$, on déduit que la densité des paires de nombres consécutifs premiers est $1/(\log n)^2$, alors qu'elle est nulle, puisque, quel que soit p , l'un des deux nombres p ou $p+1$ est pair.

G. Hardy et J. Littlewood ont proposé une conjecture (toujours non prouvée, bien sûr) selon laquelle le nombre noté $\pi_2(m)$ de nombres premiers jumeaux inférieurs à m est approché par la formule : $\pi_2(m) \approx 2 C_2 m / (\log m)^2$, où C_2 est la constante des nombres premiers jumeaux. Dans la formule définissant C_2 , les nombres p sont premiers : $C_2 = (1-1/2^2)(1-1/4^2)(1-1/6^2)\dots(1-1/(p-1)^2)\dots = 0,6601618158468695739278121\dots$

On pourrait être tenté de rire du culot des mathématiciens : incapables de montrer qu'il y a une infinité de nombres premiers jumeaux, ils énoncent des résultats considérablement plus forts (donc plus difficiles) concernant leur répartition ! Leur attitude est celle d'un alpiniste qui, après avoir échoué dans l'ascension du Mont Blanc, annoncerait : «Ça ne fait rien, ma prochaine escalade sera l'Everest.» Ce culot est cependant justifié : en mathématiques, il est souvent arrivé qu'on aboutisse dans une recherche en prouvant un théorème beaucoup plus général et plus fort que celui que l'on visait initiale-

2. LES NOMBRES PREMIERS JUMEAUX

(a) Nombres premiers et premiers jumeaux jusqu'à 2000

Les nombres premiers jumeaux sont séparés de deux unités. La conjecture des nombres premiers jumeaux affirme qu'il y en a une infinité. On a proposé une conjecture précise : il y en aurait environ $1,32 n / (\log n)^2$ parmi les nombres inférieurs à n .

2	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137
149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281	283	293	307	311	313	317
331	337	347	349	353	359	367	373	379	383	389	397	401	409	419	421
431	433	439	443	449	457	461	463	467	473	479	487	491	499	503	509
521	523	541	547	557	563	569	577	587	593	599	607	613	617	641	643
647	653	659	661	673	677	683	691	701	709	719	727	733	739	743	751
757	761	769	773	787	797	809	811	821	829	839	859	863	877		
881	887	907	911	919	929	937	941	947	953	967	971	977	983	991	997
1009	1013	1019	1021	1031	1033	1039	1043	1049	1051	1057	1063	1069	1073	1079	1087
1091	1093	1103	1107	1117	1123	1129	1133	1139	1147	1151	1153	1163	1171	1181	1187
1193	1201	1213	1217	1223	1229	1231	1237	1249	1259	1277	1283	1289	1291	1297	1301
1303	1307	1319	1321	1327	1331	1337	1343	1349	1351	1357	1361	1367	1373	1381	1399
1409	1423	1427	1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493
1499	1511	1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607	1609
1613	1619	1621	1627	1637	1657	1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811	1823	1831	1847	1861	1867	1871
1873	1877	1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987	1993	1997
1999	2003														

(b) Raréfaction des nombres premiers jumeaux

	nombres de nombres premiers	nombres de premiers jumeaux	pourcentages de premiers jumeaux
10^3	168	20	11,90
10^4	1229	205	16,68
10^5	592	1224	12,76
10^6	8498	8169	10,41
10^7	64579	58980	8,87
10^8	761455	440312	7,65
10^9	6847534	3424506	6,73
10^{10}	55052511	27412679	6,02
10^{11}	4118054813	224376048	5,45
10^{12}	31697322680	1670000000	5,27
10^{13}	246065526820	15824664872	4,56
10^{14}	204941750802	135780321665	4,22
10^{15}	19844570422669	1177209242304	3,94

(c) Les plus grandes paires de premiers jumeaux connues

835 35 × 39014 ±1	11751 chiffres	Ballinger et Gallot 1998
242 0608 × 23880 ±1	11713 chiffres	Jarai et Indlekofer 1995
408 3037 × 23356 ±1	6696 chiffres	Lifchitz et Gallot 1998
361 0005 × 239020 ±1	11755 chiffres	Lifchitz 1999

(d) Caractérisations et formules

n est le premier élément d'une paire de nombres premiers jumeaux si et seulement si :

- $4((n-1)! + 1) + n$ est un multiple de $n(n+2)$
- ou $(n-1)!(n+2)+2n+2$ est un multiple de $n(n+2)$
- ou $(n-1)!(n-2)-2$ est un multiple de $n(n+2)$.

On en déduit que la formule suivante engendre tous les nombres premiers jumeaux quand n décrit l'ensemble des entiers ≥ 0 :

$$j(n) = 3 + n[(n+2)!(n+7)/(n+3)(n+5) - ((n+2)!(n+6)/(n+3)(n+5))].$$

(e) Polynôme qui donne tous les nombres premiers jumeaux

Lorsque les variables $a, b, c, \dots, z$ deviennent l'ensemble des entiers positifs ou nuls, les valeurs positives du polynôme suivant, dû à Christoph Baxa (et tiré de la théorie des équations diophantiennes), décrivent l'ensemble des nombres p tels que $p, p+2$ constituent une paire de premiers jumeaux :

$$\begin{aligned} & (k+2)(1-(wz+h+j-q)^2 - ((g+1)(h+j)+h-z)^2 - (p+q+z+2n-e)^2 \\ & - (e^3(e+2)(a+1)^2+1-o^2)^2 - ((a^2-1)(n+l+v)^2+1-x^2)^2 - (16(a^2-1)(n+l+v)^2+1-x^2)^2 \\ & - (((a+u^2(u^2-a))^2-1)(n+4d(n+l+v))^2+1-(x+cu)^2)^2 - ((a^2-1)l^2+1-m^2)^2 \\ & - (p+l(a-n-1)+b(2a(n+1)-(n+1)2-1)-m)^2 - (q+(n+l+v)(a-p-1) \\ & +s(2a(p+1)-(p+1)^2-1)-x)^2 - (z+pl(a-p)+t(2ap-p^2-1)-pm)^2 \\ & - (16(k+1)3(k+2)(n+1)2+1-f^2)^2 - (k+1+ia-i-l)^2 - (4g+k+10-y(k+2)(k+4))^2). \end{aligned}$$

3. NOMBRES PREMIERS Jumeaux, Cousins et SEXY : LA CONJECTURE DE POLIGNAC

Deux nombres premiers jumeaux sont écartés de 2, comme 11 et 13. Deux nombres premiers cousins sont écartés de 4 (comme 7-11 ou 13-17). S'ils sont écartés de 6 (comme 5-11, 17-23, 29-35, 41-47, 59-65, 71-77, 101-107, 127-133, 149-155, 179-185, 227-233, 251-257, 281-287, 311-317, 359-365, 431-437, 461-467, 521-527, 599-605, 677-683, 701-707, 761-767, 821-827, 851-857, 911-917, 967-973, 1031-1037, 1091-1097, 1151-1157, 1201-1207, 1271-1277, 1301-1307, 1361-1367, 1421-1427, 1481-1487, 1511-1517, 1571-1577, 1601-1607, 1661-1667, 1721-1727, 1781-1787, 1841-1847, 1901-1907, 1961-1967, 2011-2017, 2081-2087, 2141-2147, 2201-2207, 2261-2267, 2311-2317, 2369-2375, 2411-2417, 2471-2477, 2531-2537, 2591-2597, 2651-2657, 2711-2717, 2771-2777, 2831-2837, 2891-2897, 2951-2957, 3011-3017, 3071-3077, 3131-3137, 3191-3197, 3251-3257, 3311-3317, 3371-3377, 3431-3437, 3491-3497, 3551-3557, 3611-3617, 3671-3677, 3731-3737, 3791-3797, 3851-3857, 3911-3917, 3971-3977, 4031-4037, 4091-4097, 4151-4157, 4211-4217, 4271-4277, 4331-4337, 4391-4397, 4451-4457, 4511-4517, 4571-4577, 4631-4637, 4691-4697, 4751-4757, 4811-4817, 4871-4877, 4931-4937, 4991-4997, 5051-5057, 5111-5117, 5171-5177, 5231-5237, 5291-5297, 5351-5357, 5411-5417, 5471-5477, 5531-5537, 5591-5597, 5651-5657, 5711-5717, 5771-5777, 5831-5837, 5891-5897, 5951-5957, 6011-6017, 6071-6077, 6131-6137, 6191-6197, 6251-6257, 6311-6317, 6371-6377, 6431-6437, 6491-6497, 6551-6557, 6611-6617, 6671-6677, 6731-6737, 6791-6797, 6851-6857, 6911-6917, 6971-6977, 7031-7037, 7091-7097, 7151-7157, 7211-7217, 7271-7277, 7331-7337, 7391-7397, 7451-7457, 7511-7517, 7571-7577, 7631-7637, 7691-7697, 7751-7757, 7811-7817, 7871-7877, 7931-7937, 7991-7997, 8051-8057, 8111-8117, 8171-8177, 8231-8237, 8291-8297, 8351-8357, 8411-8417, 8471-8477, 8531-8537, 8591-8597, 8651-8657, 8711-8717, 8771-8777, 8831-8837, 8891-8897, 8951-8957, 9011-9017, 9071-9077, 9131-9137, 9191-9197, 9251-9257, 9311-9317, 9371-9377, 9431-9437, 9491-9497, 9551-9557, 9611-9617, 9671-9677, 9731-9737, 9791-9797, 9851-9857, 9911-9917, 9971-9977, 10031-10037, 10091-10097, 10151-10157, 10211-10217, 10271-10277, 10331-10337, 10391-10397, 10451-10457, 10511-10517, 10571-10577, 10631-10637, 10691-10697, 10751-10757, 10811-10817, 10871-10877, 10931-10937, 10991-10997, 11051-11057, 11111-11117, 11171-11177, 11231-11237, 11291-11297, 11351-11357, 11411-11417, 11471-11477, 11531-11537, 11591-11597, 11651-11657, 11711-11717, 11771-11777, 11831-11837, 11891-11897, 11951-11957, 12011-12017, 12071-12077, 12131-12137, 12191-12197, 12251-12257, 12311-12317, 12371-12377, 12431-12437, 12491-12497, 12551-12557, 12611-12617, 12671-12677, 12731-12737, 12791-12797, 12851-12857, 12911-12917, 12971-12977, 13031-13037, 13091-13097, 13151-13157, 13211-13217, 13271-13277, 13331-13337, 13391-13397, 13451-13457, 13511-13517, 13571-13577, 13631-13637, 13691-13697, 13751-13757, 13811-13817, 13871-13877, 13931-13937, 13991-13997, 14051-14057, 14111-14117, 14171-14177, 14231-14237, 14291-14297, 14351-14357, 14411-14417, 14471-14477, 14531-14537, 14591-14597, 14651-14657, 14711-14717, 14771-14777, 14831-14837, 14891-14897, 14951-14957, 15011-15017, 15071-15077, 15131-15137, 15191-15197, 15251-15257, 15311-15317, 15371-15377, 15431-15437, 15491-15497, 15551-15557, 15611-15617, 15671-15677, 15731-15737, 15791-15797, 15851-15857, 15911-15917, 15971-15977, 16031-16037, 16091-16097, 16151-16157, 16211-16217, 16271-16277, 16331-16337, 16391-16397, 16451-16457, 16511-16517, 16571-16577, 16631-16637, 16691-16697, 16751-16757, 16811-16817, 16871-16877, 16931-16937, 16991-16997, 17051-17057, 17111-17117, 17171-17177, 17231-17237, 17291-17297, 17351-17357, 17411-17417, 17471-17477, 17531-17537, 17591-17597, 17651-17657, 17711-17717, 17771-17777, 17831-17837, 17891-17897, 17951-17957, 18011-18017, 18071-18077, 18131-18137, 18191-18197, 18251-18257, 18311-18317, 18371-18377, 18431-18437, 18491-18497, 18551-18557, 18611-18617, 18671-18677, 18731-18737, 18791-18797, 18851-18857, 18911-18917, 18971-18977, 19031-19037, 19091-19097, 19151-19157, 19211-19217, 19271-19277, 19331-19337, 19391-19397, 19451-19457, 19511-19517, 19571-19577, 19631-19637, 19691-19697, 19751-19757, 19811-19817, 19871-19877, 19931-19937, 19991-19997, 20051-20057, 20111-20117, 20171-20177, 20231-20237, 20291-20297, 20351-20357, 20411-20417, 20471-20477, 20531-20537, 20591-20597, 20651-20657, 20711-20717, 20771-20777, 20831-20837, 20891-20897, 20951-20957, 21011-21017, 21071-21077, 21131-21137, 21191-21197, 21251-21257, 21311-21317, 21371-21377, 21431-21437, 21491-21497, 21551-21557, 21611-21617, 21671-21677, 21731-21737, 21791-21797, 21851-21857, 21911-21917, 21971-21977, 22031-22037, 22091-22097, 22151-22157, 22211-22217, 22271-22277, 22331-22337, 22391-22397, 22451-22457, 22511-22517, 22571-22577, 22631-22637, 22691-22697, 22751-22757, 22811-22817, 22871-22877, 22931-22937, 22991-22997, 23051-23057, 23111-23117, 23171-23177, 23231-23237, 23291-23297, 23351-23357, 23411-23417, 23471-23477, 23531-23537, 23591-23597, 23651-23657, 23711-23717, 23771-23777, 23831-23837, 23891-23897, 23951-23957, 24011-24017, 24071-24077, 24131-24137, 24191-24197, 24251-24257, 24311-24317, 24371-24377, 24431-24437, 24491-24497, 24551-24557, 24611-24617, 24671-24677, 24731-24737, 24791-24797, 24851-24857, 24911-24917, 24971-24977, 25031-25037, 25091-25097, 25151-25157, 25211-25217, 25271-25277, 25331-25337, 25391-25397, 25451-25457, 25511-25517, 25571-25577, 25631-25637, 25691-25697, 25751-25757, 25811-25817, 25871-25877, 25931-25937, 25991-25997, 26051-26057, 26111-26117, 26171-26177, 26231-26237, 26291-26297, 26351-26357, 26411-26417, 26471-26477, 26531-26537, 26591-26597, 26651-26657, 26711-26717, 26771-26777, 26831-26837, 26891-26897, 26951-26957, 27011-27017, 27071-27077, 27131-27137, 27191-27197, 27251-27257, 27311-27317, 27371-27377, 27431-27437, 27491-27497, 27551-27557, 27611-27617, 27671-27677, 27731-27737, 27791-27797, 27851-27857, 27911-27917, 27971-27977, 28031-28037, 28091-28097, 28151-28157, 28211-28217, 28271-28277, 28331-28337, 28391-28397, 28451-28457, 28511-28517, 28571-28577, 28631-28637, 28691-28697, 28751-28757, 28811-28817, 28871-28877, 28931-28937, 28991-28997, 29051-29057, 29111-29117, 29171-29177, 29231-29237, 29291-29297, 29351-29357, 29411-29417, 29471-29477, 29531-29537, 29591-29597, 29651-29657, 29711-29717, 29771-29777, 29831-29837, 29891-29897, 29951-29957, 30011-30017, 30071-30077, 30131-30137, 30191-30197, 30251-30257, 30311-30317, 30371-30377, 30431-30437, 30491-30497, 30551-30557, 30611-30617, 30671-30677, 30731-30737, 30791-30797, 30851-30857, 30911-30917, 30971-30977, 31031-31037, 31091-31097, 31151-31157, 31211-31217, 31271-31277, 31331-31337, 31391-31397, 31451-31457, 31511-31517, 31571-31577, 31631-31637, 31691-31697, 31751-31757, 31811-31817, 31871-31877, 31931-31937, 31991-31997, 32051-32057, 32111-32117, 32171-32177, 32231-32237, 32291-32297, 32351-32357, 32411-32417, 32471-32477, 32531-32537, 32591-32597, 32651-32657, 32711-32717, 32771-32777, 32831-32837, 32891-32897, 32951-32957, 33011-33017, 33071-33077, 33131-33137, 33191-33197, 33251-33257, 33311-33317, 33371-33377, 33431-33437, 33491-33497, 33551-33557, 33611-33617, 33671-33677, 33731-33737, 33791-33797, 33851-33857, 33911-33917, 33971-33977, 34031-34037, 34091-34097, 34151-34157, 34211-34217, 34271-34277, 34331-34337, 34391-34397, 34451-34457, 34511-34517, 34571-34577, 34631-34637, 34691-34697, 34751-34757, 34811-34817, 34871-34877, 34931-34937, 34991-34997, 35051-35057, 35111-35117, 35171-35177, 35231-35237, 35291-35297, 35351-35357, 35411-35417, 35471-35477, 35531-35537, 35591-35597, 35651-35657, 35711-35717, 35771-35777, 35831-35837, 35891-35897, 35951-35957, 36011-36017, 36071-36077, 36131-36137, 36191-36197, 36251-36257, 36311-36317, 36371-36377, 36431-36437, 36491-36497, 36551-36557, 36611-36617, 36671-36677, 36731-36737, 36791-36797, 36851-36857, 36911-36917, 36971-36977, 37031-37037, 37091-37097, 37151-37157, 37211-37217, 37271-37277, 37331-37337, 37391-37397, 37451-37457, 37511-37517, 37571-37577, 37631-37637, 37691-37697, 37751-37757, 37811-37817, 37871-37877, 37931-37937, 37991-37997, 38051-38057, 38111-38117, 38171-38177, 38231-38237, 38291-38297, 38351-38357, 38411-38417, 38471-38477, 38531-38537, 38591-38597, 38651-38657, 38711-38717, 38771-38777, 38831-38837, 38891-38897, 38951-38957, 39011-39017, 39071-39077, 39131-39137, 39191-39197, 39251-39257, 39311-39317, 39371-39377, 39431-39437, 39491-39497, 39551-39557, 39611-39617, 39671-39677, 39731-39737, 39791-39797, 39851-39857, 39911-39917, 39971-39977, 40031-40037, 40091-40097, 40151-40157, 40211-40217, 40271-40277, 40331-40337, 40391-40397, 40451-40457, 40511-40517, 40571-40577, 40631-40637, 40691-40697, 40751-40757, 40811-40817, 40871-40877, 40931-40937, 40991-40997, 41051-41057, 41111-41117, 41171-41177, 41231-41237, 41291-41297, 41351-41357, 41411-41417, 41471-41477, 41531-41537, 41591-41597, 41651-41657, 41711-41717, 41771-41777, 41831-41837, 41891-41897, 41951-41957, 42011-42017, 42071-42077, 42131-42137, 42191-42197, 42251-42257, 42311-42317, 42371-42377, 42431-42437, 42491-42497, 42551-42557, 42611-42617, 42671-42677, 42731-42737, 42791-42797, 42851-42857, 42911-42917, 42971-42977, 43031-43037, 43091-43097, 43151-43157, 43211-43217, 43271-43277, 43331-43337, 43391-43397, 43451-43457, 43511-43517, 43571-43577, 43631-43637, 43691-43697, 43751-43757, 43811-43817, 43871-43877, 43931-43937, 43991-43997, 44051-44057, 44111-44117, 44171-44177, 44231-44237, 44291-44297, 44351-44357, 44411-44417, 44471-44477, 44531-44537, 44591-44597, 44651-44657, 44711-44717, 44771-44777, 44831-44837, 44891-44897, 44951-44957, 45011-45017, 45071-45077, 45131-45137, 45191-45197, 45251-45257, 45311-45317, 45371-45377, 45431-45437, 45491-45497, 45551-45557, 45611-45617, 45671-45677, 45731-45737, 45791-45797, 45851-45857, 45911-45917, 45971-45977, 46031-46037, 46091-46097, 46151-46157, 46211-46217, 46271-46277, 46331-46337, 46391-46397, 46451-46457, 46511-46517, 46571-46577, 46631-46637, 46691-46697, 46751-46757, 46811-46817, 46871-46877, 46931-46937, 46991-46997, 47051-47057, 47111-47117, 47171-47177, 47231-47237, 47291-47297, 47351-47357, 47411-47417, 47471-47477, 47531-47537, 47591-47597, 47651-47657, 47711-47717, 47771-47777, 47831-47837, 47891-47897, 47951-47957, 48011-48017, 48071-48077, 48131-48137, 48191-48197, 48251-48257, 48311-48317, 48371-48377, 48431-48437, 48491-48497, 48551-48557, 48611-48617, 48671-48677, 48731-48737, 48791-48797, 48851-48857, 48911-48917, 48971-48977, 49031-49037, 49091-49097, 49151-49157, 49211-49217, 49271-49277, 49331-49337, 49391-49397, 49451-49457, 49511-49517, 49571-49577, 49631-49637, 49691-49697, 49751-49757, 49811-49817, 49871-49877, 49931-49937, 49991-49997, 50051-50057, 50111-50117, 50171-50177, 50231-50237, 50291-50297, 50351-50357, 50411-50417, 50471-50477, 50531-50537, 50591-50597, 50651-50657, 50711-50717, 50771-50777, 50831-50837, 50891-50897, 50951-50957, 51011-51017, 51071-51077, 51131-51137, 51191-51197, 51251-51257, 51311-51317, 51371-51377, 51431-51437, 51491-51497, 51551-51557, 51611-51617, 51671-51677, 51731-51737, 51791-51797, 51851-51857, 51911-51917, 51971-51977, 52031-52037, 52091-52097, 52151-52157, 52211-52217, 52271-52277, 52331-52337, 52391-52397, 52451-52457, 52511-52517, 52571-52577, 52631-52637, 52691-52697, 52751-52757, 52811-52817, 52871-52877, 52931-52937, 52991-52997, 53051-53057, 53111-53117, 53171-53177, 53231-53237, 53291-53297, 53351-53357, 53411-53417, 53471-53477, 53531-53537, 53591-53597, 53651-53657, 53711-53717, 53771-53777, 53831-53837, 53891-53897, 53951-53957, 54011-54017, 54071-54077, 54131-54137, 54191-54197, 54251-54257, 54311-54317, 54371-54377, 54431-54437, 54491-54497, 54551-54557, 54611-54617, 54671-54677, 54731-54737, 54791-54797, 54851-54857, 54911-54917, 54971-54977, 55031-55037, 55091-55097, 55151-55157, 55211-55217, 55271-55277, 55331-55337, 55391-55397, 55451-55457, 55511-55517, 55571-55577, 55631-55637, 55691-55697, 55751-55757, 55811-55817, 55871-55877, 55931-55937, 55991-55997, 56051-56057, 56111-56117, 56171-56177, 56231-56237, 56291-56297, 56351-56357, 56411-56417, 56471-56477, 56531-56537, 56591-56597, 56651-56657, 56711-56717, 56771-56777, 56831-56837, 56891-56897, 56951-56957, 57011-57017, 57071-57077, 57131-57137, 57191-57197, 57251-57257, 57311-57317, 57371-57377, 57431-57437, 57491-57497, 57551-

un nombre premier jumeau, alors la série des inverses des nombres premiers jumeaux serait infinie, comme la série des inverses des nombres premiers (car l'infini divisé par 100 est encore l'infini). Donc moins d'un nombre premier sur 100 est un nombre premier jumeau. Ce qui vient d'être dit pour 100 peut être répété avec 1 000, 10 000, etc. Il y a bien raréfaction : en allant assez loin, la proportion des nombres premiers jumeaux parmi les nombres premiers tend vers 0.

Il résulte qu'il y a des séquences de plus en plus longues de nombres premiers consécutifs ne comportant aucun nombre premier jumeau. Ce résultat est à rapprocher de celui qui énonce qu'il y a des séquences de nombres composés successifs aussi longues qu'on veut : en effet, par exemple, il n'y a aucun nombre premier entre $N! + 2$ et $N! + N$ (en effet, $N! + 2$ est multiple de 2 ; $N! + 3$ multiple de 3 ; etc.).

Que la série des inverses des premiers jumeaux converge est intéressant, mais cela n'indique évidemment pas qu'il y a nécessairement une infinité de nombres premiers jumeaux : la série peut avoir une valeur finie parce que le nombre de ses termes est fini, ou parce qu'ils sont de plus en plus petits. La valeur de la série $(1/3 + 1/5) + (1/5 + 1/7) + (1/11 + 1/19) + \dots$ se dénomme B , la constante de V. Brun.

Cette constante B est particulièrement difficile à évaluer, et l'on ne connaît pas d'autres méthodes pour la calculer que d'utiliser directement sa définition : il faut donc aller très loin dans le calcul des nombres premiers.

La constante de V. Brun a été estimée par Daniel Shanks et John Wrench en 1974 (qui furent aussi les premiers à calculer 100 000 décimales du nombre π , en 1961), puis par Richard Brent en 1976. Le calcul de D. Shanks et J. Wrench utilisa les deux premiers millions de nombres premiers : celui de R. Brent prit en considération les nombres jusqu'à 100 milliards : ils dénombrent 224 376 048 nombres premiers jumeaux ! Plus récemment, le calcul a été poussé plus avant par M. Kutrib et J. Richstein, et indépendamment par Thomas Nicely, ce dernier étant au centre d'une aventure dont le récit va nous plonger dans le monde des erreurs informatiques.

THOMAS NICELY ET LE PENTIUM D'INTEL

T. Nicely est professeur au Lynchburg College, en Virginie, aux États-Unis. Il mène des recherches en théorie « computationnelle » des nombres et s'intéresse particulièrement aux nombres premiers. Souhaitant améliorer la précision de la constante de V. Brun, il lança en 1994 une série de calculs fondée sur l'énumé-

4. LES CONSTELLATIONS

À l'exception de 3, 5, 7, trois nombres premiers consécutifs ne peuvent être de la forme $[p, p+2, p+4]$; en revanche, $[p, p+2, p+6]$ et $[p, p+4, p+6]$ sont des formes possibles pour trois nombres premiers consécutifs. Pour quatre nombres premiers, $[p, p+2, p+6, p+8]$ est possible. C'est ce que l'on dénomme les constellations, et l'on conjecture que, pour chacune, il y a une infinité de nombres premiers.

Hardy et Littlewood ont donné une version numérique de la conjecture des constellations qui précise leur densité. Cette conjecture semble numériquement vérifiée.

Les trois plus grands triplets-premiers connus, tous découverts en 1998, sont : $3434471, 643960930(2^{3567}-2^{1189})-6 \times 2^{1189}-7, \dots$ (1091 chiffres, T. Forbes) $2387382, 365759390(2^{3567}-2^{1189})-6 \times 2^{1189}-5, \dots$ (1091 chiffres, T. Forbes) $2083408, 158360750(2^{3567}-2^{1189})-6 \times 2^{1189}-5, \dots$ (1091 chiffres, T. Forbes) Le site internet de Tony Forbes, <http://www.kz.demon.co.uk/ktuplets.htm> donne les mises à jour des records actuels pour les constellations, les triplets, les quadruplets, etc.

ration des nombres premiers et des nombres premiers jumeaux inférieurs à 10^{15} . À cause du coût des mémoires informatiques (il en faut énormément pour aller jusqu'à 10^{15}), son calcul se déroulait par tranches ; quand il passait d'une tranche à la suivante, il effaçait les nombres premiers calculés après en avoir extrait les informations qui l'intéressaient (il est plus facile de calculer des nombres premiers que de les stocker !). La séparation en tranches lui a permis aussi de répartir son calcul sur de nombreux ordinateurs qu'il faisait travailler pour lui dès que leurs propriétaires les laissaient inoccupés (technique qui est devenue classique pour mener de longs calculs).

De façon à garantir les résultats, T. Nicely, comme il est d'usage dans ces domaines, effectuait de nombreux contrôles : calculs effectués plusieurs fois, recoupements de méthodes indépendantes, etc. Notons que, dans l'absolu, même après contrôles, nul ne peut exclure qu'il subsiste encore une erreur. Il se peut, par exemple, que deux erreurs dans deux calculs différents produisent le même résultat... erroné. Cette possibilité est cependant jugée très improbable, et l'on néglige une telle éventualité. Comme toujours en sciences expérimentales, la probabilité d'erreur peut être rendue faible, voire très faible, mais jamais totalement nulle.

Lors de son calcul, T. Nicely, à sa grande déception, trouva une anomalie. Quelque chose clochait, car deux résultats qui auraient dû coïncider étaient différents. Dans un tel cas (fréquent !), le programmeur commence par soupçonner (a) le programme, puis, dans l'ordre, (b) le compilateur ; (c) d'éventuels virus ; (d) le système d'exploitation et seulement enfin (e) le matériel : mémoires, bus de données ou microprocesseur. On n'en arrive pratiquement jamais à l'étape (e), car on a trouvé l'erreur avant ou, assez fréquemment, elle a disparu quand on a

modifié le programme sans que personne ne comprenne bien pourquoi ! Les causes matérielles peuvent être particulières à votre machine (saleté sur un de vos circuits, composants défectueux) ou générales : erreur dans la conception ou le dessin d'un circuit. L'erreur aléatoire provoquée par un rayon cosmique inopportun ou une charge électrique parasite qui fait basculer un circuit ne sont pas à exclure mais elles sont quasi impossibles à diagnostiquer rétrospectivement.

L'anomalie décelée par T. Nicely refusait de disparaître : aucune des causes simples envisagées ne semblait responsable. Après plusieurs semaines de recherche durant lesquelles T. Nicely avait fait exécuter la partie du programme d'où semblait provenir l'erreur sur un processeur plus ancien (un 486 d'Intel), il assista à l'interloqué à sa disparition. En décortiquant alors de près sa découverte, il aboutit (quatre mois après la détection de l'erreur) à la certitude que c'était le *Pentium* d'Intel qui était la cause du mal. Celui-ci évaluait faussement l'inverse des nombres premiers jumeaux : 824 633 702 441 et 824 633 702 443, l'évaluation étant faussée dès la dixième chiffre !

Après avoir averti la Société Intel, qui ne répondit pas, il informa ses collègues de l'erreur et la nouvelle se répandit dans le monde entier comme une traînée de poudre, obligeant Intel à réagir. Intel reconnut avoir eu connaissance de l'erreur mais ne pouvait échanger toutes les puces défectueuses (plus de cinq millions en avaient été vendues, et même le puissant Intel n'aurait pu supporter le coût d'un remplacement systématique). Seuls les acheteurs pouvant attester que le type d'erreurs détectées dans certaines divisions étaient graves pour eux purent obtenir la puce de remplacement (quand elle fut rendue disponible). Il en résulte que la puce de nombreux ordinateurs encore en service (fabriqués en 1994 et

1995) reste défectueuse (voir la figure 1, qui vous permet de savoir si vous êtes concerné). Si cette imperfection est sans importance pour faire courir et sauter Lara Croft ou pour le bon fonctionnement d'un traitement de texte, il n'en est pas ainsi pour ceux qui utilisent un tableur ou un logiciel de statistiques.

L'argument avancé par Intel que l'erreur ne se produit qu'une fois tous les 27 000 ans pour un utilisateur moyen faisant 1 000 divisions par jour est contestable. D'une part, un utilisateur de tableur de logiciel scientifique ou de comptabilité fait beaucoup plus de 1 000 divisions par jour ; d'autre part, le taux d'erreurs du Pentium est dix millions de fois supérieur à la norme admise dans le monde des processeurs. Les ingénieurs d'Intel avaient commis une bourde dans la paitie de la puce servant à faire les divisions, et cette erreur, gravée au plus profond de cinq millions de puces disséminées dans le monde entier, était vraiment ennuyeuse, quoi que prétende Intel.

Un analyste financier trouva des cas où le quatrième chiffre d'un résultat était faux. Un expert médical affirma que : «Toute erreur un tant soit peu significative dans une analyse de résultats est susceptible d'entraîner des conséquences sur la vie et la mort». Pendant plusieurs mois, Intel fut l'objet de moqueries qui circulaient sur le réseau : «Combien de concepteurs du Pentium faut-il pour visser une ampoule ? Réponse : 1,999904274, mais c'est une bonne approximation pour un non technicien». «Pourquoi Intel a-t-il préféré le terme Pentium plutôt que 586 qui venait naturellement après le processeur 486 ? Parce qu'il a additionné 486 avec 100 en utilisant le Pentium et qu'il a trouvé 585 999990132», etc.

Les puces vendues aujourd'hui sont bien sûr exemptes du défaut qu'Intel a appris à réparer avant d'en vendre des millions : si votre machine est récente, vous n'avez rien à craindre.

L'ARITHMÉTIQUE JUSTIFIÉE ?

La découverte d'une telle erreur lors d'un calcul sur les nombres premiers a été saluée par de nombreux mathématiciens comme une preuve de leur propre utilité : il n'est pas absurde de mener de longs calculs arithmétiques qui nousent dans leurs retranchements les différents composants matériels et logiciels d'une machine, du processeur jusqu'au compilateur, et permettent de découvrir des erreurs qui, sinon, passeraient inaperçues.

Je ne pense pas que cela soit très sérieux. Il serait triste que les mathématiciens ne puissent justifier leur existence que par de tels exploits. On devrait affirmer que : «Les microprocesseurs sont

utiles, car ils servent à faire de bonnes mathématiques», plutôt que l'inverse : «Les mathématiques sont utiles, car elles servent à faire de bons microprocesseurs.»

C'est la tentation, quelque peu scandaleuse, d'Intel de cacher ce qu'il savait qui a été dévoilée, et elle ne l'a été que parce que T. Nicely n'a pas renoncé à identifier la cause d'erreur. C'est finalement l'existence du monde universitaire, avec sa liberté, son esprit de curiosité et son exigence de rigueur poussée parfois jusqu'à l'absurde qui fut à l'origine de la découverte du camouflage. Une entreprise industrielle ou commerciale aurait-elle accepté qu'un de ses employés découvrait un problème – plutôt bénin – dans un programme mène la recherche de l'erreur plusieurs mois de suite jusqu'à la recherche dans le microprocesseur ?

LES ÉCARTS ENTRE NOMBRES PREMIERS

L'objectif «premier» de T. Nicely était l'identification des records d'écarts entre nombres premiers. On sait que deux nombres premiers consécutifs peuvent être très écartés l'un de l'autre. Beaucoup plus difficile est de savoir quand un écart donné se produit pour la première fois.

La première fois que l'écart 6 apparaît est après 23, car 24, 25, 26, 27 et 28 sont composés pour mesurer un écart, on considère la différence entre les deux nombres premiers qui encadrent les nombres composés consécutifs, 23 et 29 dans notre exemple). La première fois qu'apparaît l'écart 110 est après 370261. Aujourd'hui, grâce au programme de T. Nicely, on sait que la première fois que l'écart 906 apparaît, c'est après 218209405436543, et 906 est le plus grand nombre pour lequel on connaît cette information.

Dans son article à paraître, T. Nicely remercie Intel pour un don d'ordinateur et pour l'aide apportée par plusieurs ingénieurs d'Intel dans le perfectionnement de son programme. Sans rancune !

D. Shanks a conjecturé que la taille de la première apparition de l'écart E se produit au nombre premier $p(E) \approx \exp \sqrt{E}$. Cette conjecture a été affinée par Weintraub qui proposa après expérimentation : $p(E) \approx \exp \sqrt{1,165746 E}$. Un argument heuristique proposé par Marek Wolf conduisit à une conjecture plus fine encore : $p(E) \approx E^{1/2} \cdot \exp((\log^2(E) + 4E)^{1/2}/2)$.

Les calculs de M. Wolf et de T. Nicely confirment cette loi. Il n'est pas étonnant ici que ce soit un physicien qui propose la conjecture la plus avancée, car, comme on ne sait quasi rien démontrer sur les écarts entre nombres premiers, l'arithmétique est sur ce point une science observationnelle proche de la physique, où l'on utilise des lois (bien sûr, non démon-

trées) pour en proposer d'autres (non démontrées) qu'éventuellement on pourra confirmer ou invalider par un calcul.

UN RÉSULTAT NOUVEAU ET TRÈS SIMPLE

Signalons une magnifique découverte récente concernant les écarts entre nombres premiers, due encore à M. Wolf, cette fois associé à A. Odlyzko et M. Rubinfeld. Pour la tranche des nombres premiers qu'on explore systématiquement (aujourd'hui de 1 à environ 10^{15}), on constate que 6 est l'écart entre nombres premiers le plus fréquent. Doit-on alors penser qu'en est toujours ainsi ?

Non ! L'analyse heuristique et le calcul pour confirmation conduisent à penser qu'il y a changement du «champion» vers $1,7 \cdot 10^3$ l'écart gagnant 6 étant alors remplacé par 30. Plus loin vers $5,81 \cdot 10^{428}$, le champion devient 2 310, puis vers $1,48 \cdot 10^{656}$ devient 30 030. La règle semble être que les champions successifs sont les produits des nombres premiers : $6 = 2 \times 3$, $30 = 2 \times 3 \times 5$; $2\,310 = 2 \times 3 \times 5 \times 7$; $30\,030 = 2 \times 3 \times 5 \times 7 \times 11$; etc.

La conjecture affirmant que les choses sont réellement ainsi (c'est-à-dire qu'indéfiniment il y a changement des champions, qui sont successivement tous les produits de nombres premiers) est tellement évidente de tout ce qu'on sait démontrer qu'on peut se dispenser de l'étude de l'écart entre nombres premiers les mathématiciens ont de quoi s'occuper quelques siècles, voire un millénaire entier.

Jean-Paul DELAHAYE est professeur à l'Université de Lille. Adresse internet : delahaye@fl.fr

C. C. LDWELL, *The Prime Pages*. <http://www.utm.edu/research/primess/>

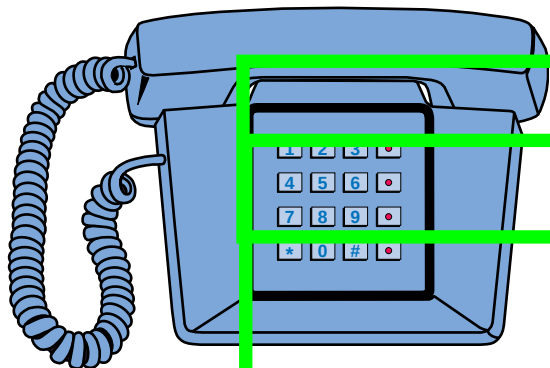
T. NICELEY, *Prime k-tuplets*. <http://www.ltkz.demon.co.uk/ktuplets.htm>

J. M. MULLER, *Algorithmes de division pour microprocesseurs : illustration à l'aide du «Bug» du Pentium, Technique et science informatiques*, 14-8, pp. 1031-1049, 1985.

T. NICELEY, *Pentium Division Flaw*. <http://www.lynchburg.edu/public/academic/math/nicely/pentium/division.htm>

T. NICELEY, *Enumeration to $1e14$ of the Twin Primes and Brun Constant*, in *Virginia Journal Science*, 40-3, pp. 193-204, 1990. <http://www.lynchburg.edu/public/academic/math/nicely/twins/twins.htm>

T. NICELEY, *New Maximal Prime Gaps and First Occurrences, Mathematics of Computation*, 1999 (article à paraître). <http://www.lynchburg.edu/public/academic/math/nicely/gaps/gaps.htm>



Tours, tortillements, topologie et téléphone

IAN STEWART

L'ADN s'entortille comme un cordon de téléphone.

Pourquoi le cordon du téléphone s'entortille-t-il sans cesse? Lors des premières utilisations, cette spirale hélicoïdale qui relie le combiné à son berceau pend sans fantaisie, mais, les semaines passant, elle devient désagréablement entortillée. On observe le même comportement avec un élastique dont on tient les extrémités entre le pouce et l'index de chaque main ; quand on fait rouler l'élastique entre les doigts, il s'enroule, puis se surenroule. Le phénomène est général : les biologistes le retrouvent même quand ils étudient l'ADN.

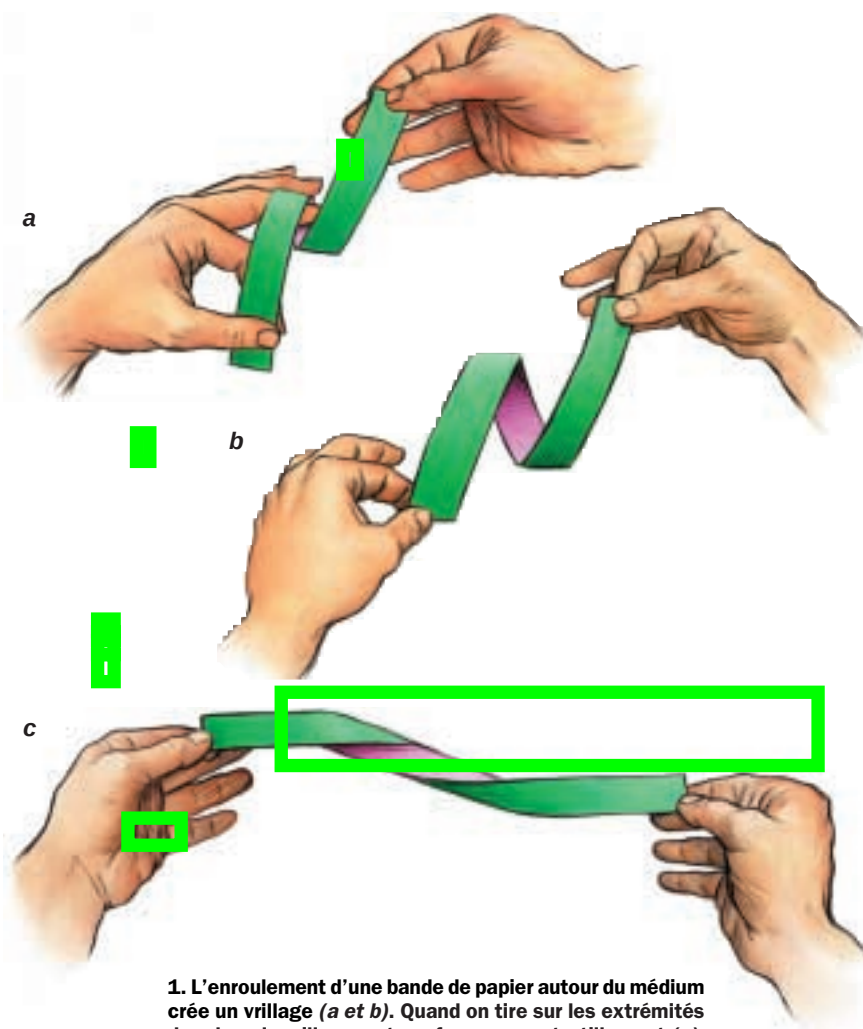
Pourquoi le surenroulement? Quand le téléphone sonne, je le prends de la main droite et le tourne de 90 degrés. Puis, pour parler, je passe souvent le combiné dans la main gauche, libérant la droite pour écrire ; au cours de ce transfert, le combiné tourne de 180 degrés. Enfin, la conversation terminée, je raccroche l'appareil de la main gauche, ajoutant encore un tortillement de 90 degrés. Ainsi, quand je téléphone, j'inflige généralement au cordon un tour complet sur lui-même, toujours dans le même sens.

Si j'ai conservé le combiné dans la main droite, je déroulerais le cordon en le reposant ; c'est le transfert dans la main gauche qui est responsable de l'effet observé. On retrouve d'ailleurs ce même effet quand on enroule un tuyau ou un long câble électrique en travers du torse, à la manière des alpinistes : progressivement le câble s'entortille. Quelque chose transforme les vrillages en tortillements, mais quoi?

La branche des mathématiques qui explore ces phénomènes est la topologie, la géométrie des objets déformables, celle des transformations continues. Les topologistes distinguent deux manières de faire une boucle dans un ruban plat : les tortillements et le vrillage. Pour saisir la différence, utilisons une bande de papier forte de 20 centimètres de long et de 2 centimètres de large. Colorions une face en vert, et une face en violet, afin de les distinguer ultérieurement.

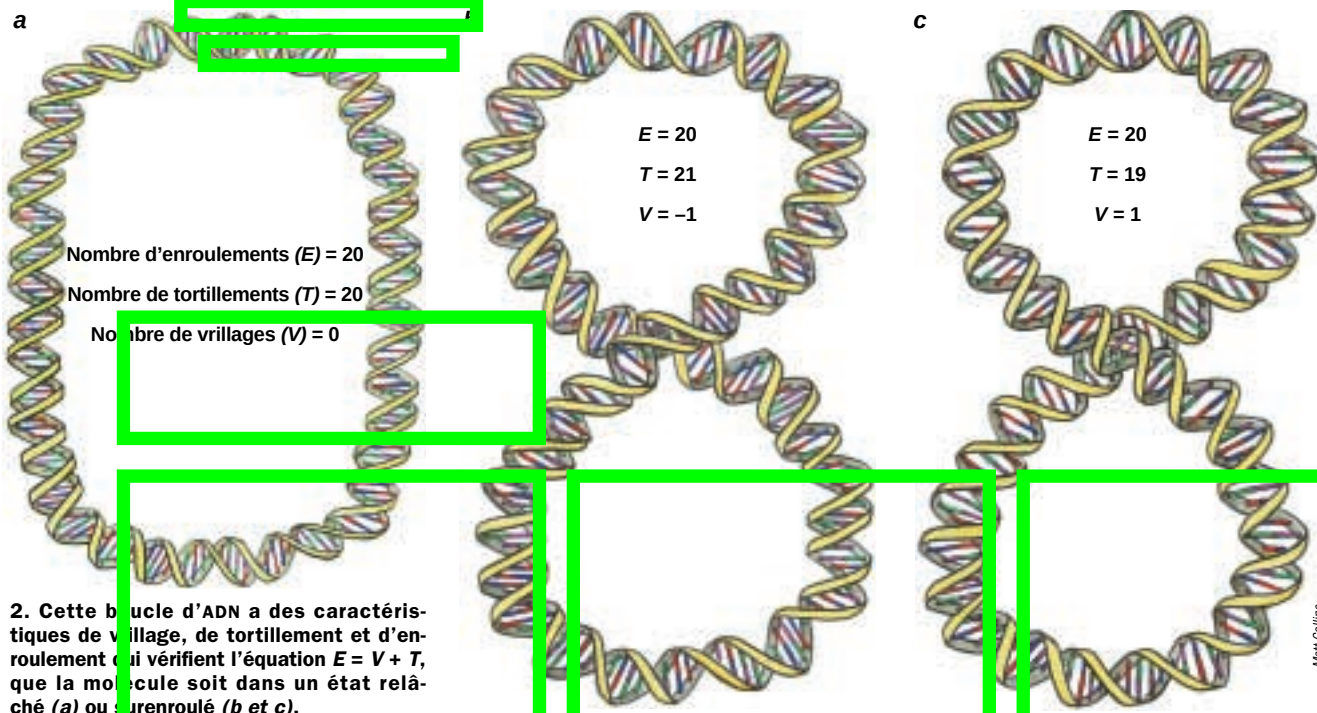
Prenons le ruban à plat entre le pouce et l'index de la main gauche ; puis, de la main droite, prenons l'extrémité libre et enroulons-la d'un tour autour du médium gauche (voir la figure 1). Retirons alors le médium pour libérer la boucle formée. Nous n'avons ainsi fait qu'un tour de ruban ; on dit que le nombre de vrillages est égal à un. Si l'on écarte lentement les mains, la bande se déforme et s'entortille. Si l'on marquait, sur la bande non vrillée, des flèches parallèles entre elles, et perpendiculaires à l'axe du ruban, on verrait que les flèches, restant perpendiculaires à l'axe du ruban, tournent autour de celui-ci d'un tour complet. Le tortillement, qui mesure la torsion du ruban, est égal à un. Autrement dit, le vrillage diminue et le tortillement augmente lorsque l'on étire le ruban vrillé. On aurait obtenu le même résultat si l'on avait tenu le ruban à plat devant soi, et si, maintenant l'extrémité gauche fixe, on avait tordu l'extrémité droite de 360 degrés. Autrement dit, le vrillage peut se transformer topologiquement en tortillement.

Vrillages et tortillements sont orientés : ils peuvent être «positifs» ou «négatifs».



1. L'enroulement d'une bande de papier autour du médium crée un vrillage (a et b). Quand on tire sur les extrémités du ruban, le vrillage se transforme en un tortillement (c).

Mart Collins



2. Cette boucle d'ADN a des caractéristiques de vrillage, de tortillement et d'enroulement qui vérifient l'équation $E = V + T$, que la molécule soit dans un état relaxé (a) ou surenroulé (b et c).

Un sens étant décrété positif, son image dans un miroir sera négative. Je propose de convenir que le vrillage représenté sur la figure 1 est positif, mais que le tortillement est négatif. De la sorte, on obtient l'équation simple : $V + T = 1$, où V est le nombre de vrillages, et T le nombre de tortillements si l'on considère que le ruban est refermé sur lui-même. En enroulant deux fois le ruban autour du médium, on lui donne deux tours positifs, ce qui engendre un tortillement égal à 1 quand on écarte les mains. Cette transformation se retrouve avec trois tours, quatre tours, etc.

On observe le même phénomène quand on tord une ficelle. Elle n'est pas plane, comme un ruban, mais il n'y a pas de raison qu'elle ne soit pas tordue ou torsadée ; là encore, le nombre de tortillements est relié au nombre de vrillages, c'est-à-dire au nombre de tours qui ont été initialement donnés. Si l'on maintient la ficelle tendue, elle ne peut présenter des tortillements, mais si nous relâchons la ficelle, nous la verrons tourner tandis que le surenroulement disparaîtra. En effet, la ficelle est légèrement élastique : on peut la tordre, mais elle exerce alors un couple en sens inverse de celui qu'on applique. Quand on supprime le couple appliqué, le couple dû à l'élasticité du matériau provoque la rotation de la ficelle jusqu'à ce que ce couple s'annule.

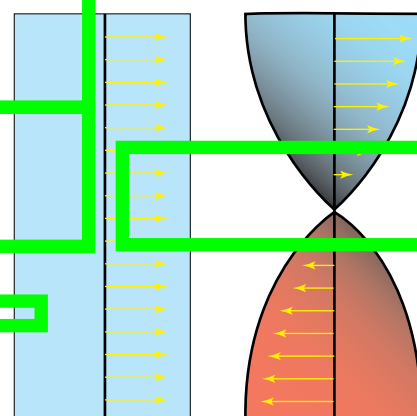
En 1883, le mathématicien britannique Alfred Greenhill expliqua pourquoi un ruban est plutôt vrillé qu'entortillé : il démontra qu'une forme vrillée contient moins d'énergie élastique que la forme

entortillée correspondante : de même, une bande de papier se vrille plutôt, sauf si l'on apporte de l'énergie en tirant les deux extrémités dans des directions opposées. Greenhill démontra que, si un cylindre infiniment long est tordu par des forces à l'infini, il flambe en formant une hélice. Récemment, D. Stump et K. Gates, de l'Université du Queensland, et W. Flasar, de l'Université de Sydney, ont calculé l'élasticité d'un cylindre tordu en utilisant des hypothèses plus réalistes. Ils ont obtenu des formules qui donnent la forme exacte du surenroulement des câbles sous-marins.

Le cordon de téléphone est plus complexe, parce qu'il est initialement torsadé. Cependant il transforme également le tortillement en vrillages, comme un simple fil, du moins si son propre enroulement

hélicoïdal ne se défait pas (on observe d'étranges défauts du cordon, dans certains cas). Pour prévoir le comportement du cordon, il est utile d'imaginer qu'il contient une longue ficelle épaisse, à l'intérieur de l'hélice, enchâssant un long ruban plat quand on tord le cordon, c'est comme si on tordait la ficelle et le ruban.

La molécule d'ADN, qui porte l'information génétique des êtres vivants, est une hélice, comme un cordon de téléphone. C'est même une double hélice : deux brins hélicoïdaux s'enroulent l'un autour de l'autre, à la façon d'une échelle qui aurait été vrillée. Les biologistes explorent le comportement de la molécule dans des conditions variées, et ils observent que la molécule subit des surenroulements, avec des transitions entre vrillage et tortillement. Comme nous l'avons vu, l'ADN et les cordons de téléphone ont les comportements que n'ont pas les ficelles : ils peuvent se désenrouler ou se surenrouler. Pour une boucle d'ADN, on décrit la structure par trois paramètres : le nombre d'enroulements E , c'est-à-dire le nombre de fois qu'un des brins croise l'autre, quand la molécule est couchée à plat sur un plan ; le nombre T de tortillements de l'ADN ; le nombre V de vrillages. Ces trois paramètres sont reliés par la formule : $E = V + T$, qui généralise la formule évoquée précédemment. Pour une boucle d'ADN, E est fixé, de sorte que la somme $V + T$ l'est aussi, mais nous pouvons changer des tortillements en tours, et inversement. La figure 2 montre ainsi des exemples avec une boucle d'ADN dont E est égal à 20.



3. Le tortillement mesure la torsion d'un ruban ; c'est le nombre de tours de flèches initialement parallèles autour de l'axe vertical (à droite, ce nombre est 1/2).

Botanique

Les Orchidées de France, Belgique et Luxembourg

Ouvrage collectif de la Société française d'Orchidophilie, sous la direction scientifique de Marcel Bournérias. Éditions Biotope, 1998.

Les orchidées émerveillent et intriguent : comment rester insensible à la beauté et au mystère de leurs fleurs ? Si les orchidées tropicales sont les plus connues du public, des orchidées sauvages peuplent des milieux variés de nos régions. Certains botanistes regroupés au sein de la Société française d'orchidophilie (SFO) se consacrent à leur étude passionnée. L'ouvrage présenté ici est ainsi le résultat d'un travail collectif de membres de la SFO, sous la responsabilité de Marcel Bournérias. Ce n'est pas seulement une flore de qualité, car, hormis l'aspect monographique et les clés de détermination, le quart de l'ouvrage se présente comme une synthèse des connaissances actuelles sur les orchidées de nos régions, leur morphologie, leur biologie étrange, leur écologie, les conditions nécessaires à leur protection, sans oublier l'histoire de l'orchidologie, ainsi que les traditions populaires.

La famille des orchidacées – c'est le terme officiel de la nomenclature actuelle – est une famille homogène, quant au plan d'organisation, mais elle est morphologiquement diversifiée. Certains genres, cependant, offrent des singularités qui leur valent d'être rangés par certains dans des familles annexes. Des formes extraordinaires existent aussi : *Disperis paludosa*, une orchidée d'Afrique du Sud, a deux sépales latéraux qui sont pourvus de profonds éperons nectarifères. Après avoir rappelé la place des orchidées dans le règne végétal et leur répartition dans le monde, les auteurs analysent leur morphologie.

Le chapitre 2 est consacré à la biologie des orchidées. Les orchidées ne peuvent vivre seules ; elles ont besoin d'être « entourées et choyées », comme si leur complexité nécessitait un travail d'équipe. Ce sont d'abord leurs relations avec des

champignons qui sont présentées : intervenant dans la germination des graines, extrêmement fines, dont la plantule n'est pas différenciée et qui sont dépourvues de réserves. Cette symbiose est confortée au cours de la vie de la plante adulte : le champignon participant aux mycorhizes contribue à la nutrition de la plante, mais cela ne va pas sans conflits : le champignon peut être phagocyté dans certaines cellules, ce qui prévient l'envahissement du reste de la plante. Dans certains genres, toutes les racines ne sont pas des mycorhizes, et certains organes restent toujours indemnes : parties aériennes, rhizomes et tubercules.

La pollinisation des orchidées constitue une remarquable histoire de coévolution, portée à son apogée avec les relations entre les onchrys et certaines espèces d'hyménoptères. Les troublantes ressemblances entre le labelle de certaines espèces et la femelle de l'hyménoptère incitent les mâles à tenter un accouplement avec la fleur, d'autant que (les auteurs n'y font qu'allusion) des substances odorantes analogues aux phéromones de l'insecte sont synthétisées par la fleur. La spécificité plante-insecte n'est cependant pas suffisante pour pré-

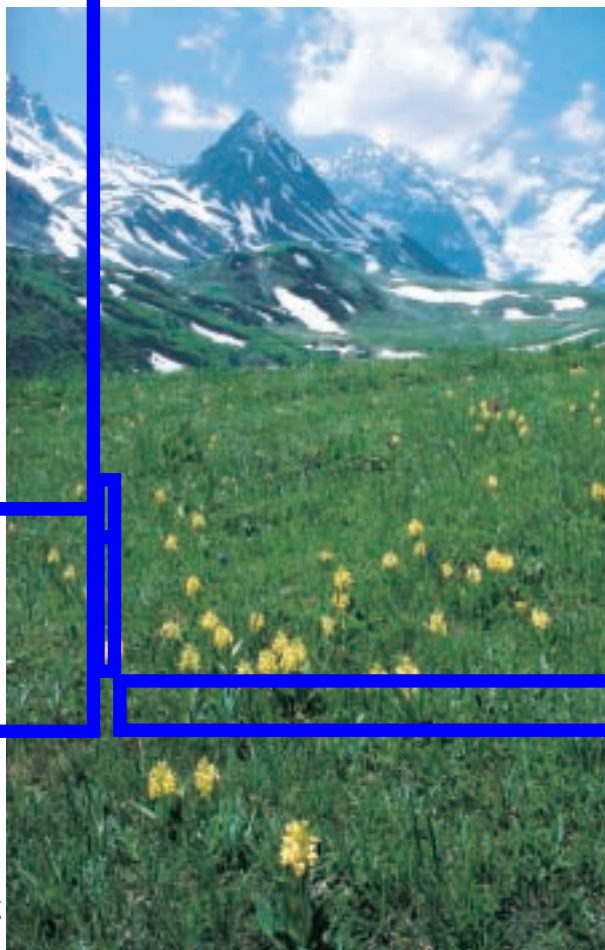
venir les hybridations entre taxons, ce qui complique la systématique. L'identification des hybrides n'est pas toujours aisée, car certains taxons parents sont présentés à une forte variation, et il est nécessaire de posséder une parfaite connaissance de cette variation pour le faire. Méthodes d'investigation et règles de nomenclature des hybrides sont présentées et discutées.

Biogéographie et écologie font l'objet du chapitre 4. Contrairement à ce que pourrait croire le profane – et ceci est vrai pour les autres plantes ! –, la répartition des orchidées sur le terrain est loin d'avoir un caractère définitif. Les causes en sont analysées, elles tiennent à la fois à la biologie de certaines espèces, aux destructions de stations, mais aussi aux progrès de la connaissance taxonomique. Il faut dire que la SFO œuvre de manière exemplaire à la connaissance biogéographique : une cartographie départementale des différentes espèces est déjà publiée pour 23 départements, et l'atlas de répartition des orchidées sauvages en est à sa troisième édition.

Les facteurs de la répartition sont ensuite envisagés selon les territoires phytogéographiques (les auteurs insistent sur les espèces endémiques, et celles qui sont en limite d'aire dans nos régions), selon l'étagement de la végétation et selon les facteurs édaphiques et microclimatiques.

Le chapitre 5 est consacré à la protection des orchidées : la régression des orchidées est inquiétante. On le voit aux chiffres présentés et aux cartes qui montrent le recul de quelques espèces en Île-de-France. Ce ne sont pas seulement les prélèvements ou les destructions de stations qui sont en cause, mais, surtout, les modifications de l'occupation et de l'utilisation du territoire, les changements de comportements, au premier rang desquels la déprise agricole et les effets de l'« agriculture productiviste ». Une notion essentielle dans la protection des espèces est celle de « solidarité écologique » entre biotopes voisins. En effet, la disparition d'une espèce n'est pas à rechercher uniquement dans son propre biotope, mais résulte fréquemment de modifications des facteurs dans des biotopes voisins.

Face à cette situation, des mesures légales de protection existent, protection des espèces et protection des milieux. Les



1. Une population de *Dactylorhiza sambucina* orne la pelouse sub-alpine au col du Lautaret (Hautes Alpes).

Photographies de Marcel Bournérias



2. La forme commune du *Dactylorhiza sambucina*, à fleurs jaunes.



3. *Dactylorhiza sambucina*, forme à fleurs rouges.

différentes modalités qui sont présentées constituent une précieuse mise au point, d'autant que la situation est envisagée aussi en Belgique et dans le grand-duché de Luxembourg, et fait aussi référence aux mesures communautaires et internationales. On est frappé par le nombre des organismes et des structures en cause, et l'on est conduit à espérer qu'ils aient en bonne coordination dans un souci d'efficacité et d'optimisation des moyens, mais force est de constater que ces actions restent souvent le fait de bénévoles ou de quasi-bénévoles...

La seconde partie de l'ouvrage est consacrée aux monographies (150 espèces et sous-espèces). Les orchidophiles ont une réputation de minutieux observateurs, ce qui les entraîne à décrire des variations minimes, contribuant ainsi à la connaissance de ce que l'on nomme aujourd'hui la «biodiversité». Toutefois certaines espèces linnéennes se sont trouvées pulvérisées en un grand nombre de taxons dont la valeur est parfois discutée. Les auteurs prennent ici le parti d'une position moyenne, entre «rassembleurs» et «diviseurs». Chaque taxon est présenté par une fiche descriptive, avec généralement plusieurs photographies de qualité, l'une présentant l'aspect général sur le terrain, les autres concer-

nant les fleurs, parfois enrichies d'une superbe illustration «pleine page». Les renseignements apportés sont les suivants : nomenclature avec synonymies, caractères morphologiques et phénologiques, répartition géographique, conditions stationnelles, mesures de protection, hybrides et diverses observations.

Au total, voici un splendide ouvrage qui, sans nul doute, deviendra la bible des orchidophiles grâce à son sérieux scientifique, à sa modernité et à sa valeur de synthèse. La remarquable richesse de l'illustration, qui met en valeur la somptuosité de ces fleurs précieuses, en fait aussi un livre destiné à toutes les personnes sensibles à la beauté de la Nature. J'espère, comme M. Aynonh, auteur de la préface, qu'il contribuera à la conservation de la diversité biologique exceptionnelle de cette famille. En patronnant la publication divers organismes s'y engagent implicitement : ministère de l'Aménagement du territoire et de l'Environnement, ministère de la Région wallonne (direction générale des ressources naturelles et de l'environnement), *Natur Musée* du Luxembourg, *Gaz de France* et Yves Rocher ! Une seule critique : osera-t-on emporter sur le terrain un si beau livre ?

Christian BOCK

Mathématiques

Œuvres de Pierre de Fermat (I. La théorie des nombres)

Textes traduits par Paul Tannery, introduits et commentés par R. Rashed, Ch. Houzel et G. Christol. Éditions Blanchard, 1998.

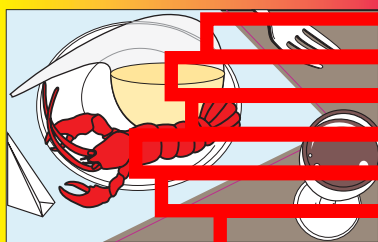
Paul Tannery est né en 1843, à Mantes. À sa sortie de l'École polytechnique, en 1865, il est nommé ingénieur des tabacs. Cependant, il reste surtout connu pour ses travaux d'historien des sciences, ayant publié essentiellement dans des revues scientifiques et philosophiques : il fut l'auteur de recherches sur l'histoire de l'astronomie grecque, il traduisit Diophante, il traduisit et commenta l'œuvre mathématique de René Descartes... Ses *Œuvres de Fermat* ont été éditées de 1891 à 1896, et un dernier volume a paru en 1912. Ces ouvrages sont depuis longtemps épuisés, et il est heureux que la Librairie Blanchard, dont on connaît le travail pour la diffusion des livres anciens, ait accepté

FRANCE INFO et POUR LA SCIENCE

vous invitent
à écouter la chronique
de Marie-Odile Monchicourt.

Info Sciences

Tous les jours
sur **France Info**
à 15 heures 41,
17 heures 10,
20 heures 12,
22 heures 12,
et 23 heures 42



Les prochains
résultats présentés
dans la rubrique
Science et Gastronomie
seront annoncés sur
France Info
le 30 juin 1999.

FRANCE

info

de publier une reproduction des textes de Tannery. La simple réédition de la traduction de Tannery aurait été déjà appréciable, car elle aurait mis à la disposition d'un large public des textes presque mythiques tant l'ombre de Pierre de Fermat plane sur toute la théorie des nombres. Toutefois Roshdi Rashed et ses collègues ne se sont pas limités à ce simple exercice ; ils ont proposé, en introduction, un bref commentaire, en langage moderne, de chacun des passages (malgré sa brièveté, cette introduction représente un quart de l'ouvrage). Ce commentaire s'adresse au lecteur profane, c'est-à-dire au lecteur qui a quelques connaissances d'arithmétique élémentaire et qui s'intéresse à l'histoire de cette science. De ce point de vue, l'ouvrage est bien dans la tendance actuelle, qui consiste à faciliter l'accès aux diverses disciplines, et, notamment, à l'histoire des mathématiques. Dans cette même veine, un deuxième tome sera consacré à la géométrie de Fermat.

Traduite en français, avec les notations d'aujourd'hui, un texte latin le rend plus accessible, mais pourquoi s'intéresser à un travail mathématique datant de plus de trois siècles et largement dépassé, puisque la plus célèbre des conjectures a été démontrée par Andrew Wiles, il y a quelques années ? L'intérêt essentiel est presque d'ordre pédagogique : la plupart des résultats de Fermat appartiennent maintenant à des théories bien élaborées et, pour aller vite à l'essentiel, les ouvrages modernes ne donnent ces résultats que comme des applications particulières des dites théories. Ils présentent ainsi les mathématiques comme une science achevée, passant sous silence toutes les recherches de cas particuliers qui, mis bout à bout, ont permis l'élaboration des théories complètes. Or il faut se frotter à de nombreux exemples pour découvrir les invariants, les bonnes transformations qui permettent de rassembler en un même ensemble toute une classe de problèmes. L'ouvrage actuel permet à l'enseignant d'illustrer les premiers chapitres de ses cours d'arithmétique, pour leur donner une perspective historique. Il peut aussi être l'occasion, à un niveau plus élémentaire, au lycée, au collège ou dans des clubs mathématiques, d'initier les élèves à l'arithmétique sans entrer dans des considérations théoriques.

Au travers de l'apport de cet ouvrage à l'histoire de l'arithmétique, on découvre les interrogations des mathématiciens de l'époque sur diverses notions. Ainsi les voit-on débattre pour savoir si 1 est ou non un nombre. Ainsi les voit-on s'interroger sur la meilleure façon d'étendre la

notion de partie aliquote, c'est-à-dire de diviseur strict d'un nombre entier, à l'ensemble des nombres fractionnaires. Ainsi les voit-on réfléchir sur la notion de nombres négatifs, qui, apparaissant comme solutions de certains problèmes, sont qualifiés de « fausses » solutions. Tous ces éléments, ces hésitations éclairent maints problèmes pédagogiques et relativisent beaucoup les erreurs des élèves ou des étudiants. N'oublions pas que les problèmes qui ont mis des siècles à émerger et à trouver une solution sont des problèmes intrinsèquement difficiles, même s'il existe aujourd'hui des théories qui les résolvent en quelques lignes.

J'espère que ce livre aidera tous ceux qui veulent simplement comprendre le pourquoi de chaque chose, y compris le pourquoi d'apprendre.

Jean LEFORT

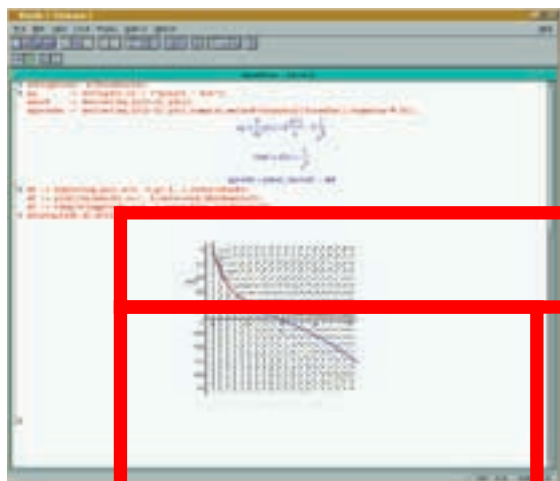
Informatique

Maths et Maple

Jean-Michel Ferrard. Éditions Dunod, 1998.

Le livre *Maths et Maple* présente un vaste ensemble d'expérimentations mathématiques que l'on peut conduire avec le logiciel *Maple* dans les classes préparatoires aux Grandes Écoles ou dans le premier cycle des universités. Outre les problèmes d'approximation des fonctions et de résolution numérique d'équations différentielles, on y trouve une présentation des techniques d'intégration approchée et de l'analyse numérique matricielle.

Je ne préjuge cependant à cet ouvrage de trop privilégier l'aspect boîte noire du logiciel, notamment en ce qui concerne les calculs formels effectués. Le professeur de mathématiques que je suis est choqué que l'on calcule la limite d'une forme indéterminée, telle $(f(a + 2h) - 2f(a + h) + f(a))/h^2$, quand h tend vers 0, par l'instruction : *limit(l'expression)*. Une telle méthode risque de laisser croire aux étudiants que l'activité mathématique se résume à appuyer sur « le bon bouton » sans chercher à comprendre quel mécanisme il déclenche pour produire le « résultat ». Un bon usage de *Maple* consisterait plutôt à ne faire effectuer par la machine que des calculs que l'utilisateur comprend et pourrait effectuer lui-même ; par exemple, pour la forme indéterminée précédente, je préférerais que l'on fasse calculer un développement



Résolution d'une équation avec le logiciel Maple.

limité du numérateur, puis que l'on simplifie la fraction.

En ce qui concerne la résolution numérique des équations différentielles, si l'on peut exposer facilement dans un cours la méthode d'Euler, et éventuellement justifier la précision médiocre de cette méthode, il n'en va pas de même pour les techniques de résolution approchée plus performantes, telles la méthode de Runge-Kutta d'ordre 4 ou la technique «prédicteur-correcteur» d'Adams-Moulton. *Maths et Maple* présente ces techniques et propose leur étude expérimentale, ainsi qu'une étude formelle de leur précision par développement limité de l'erreur sur un pas. On voit ici tout l'intérêt d'un logiciel de calcul numérique et symbolique dans l'enseignement des mathématiques.

Michel QUERCIA

Pharmacie

The Practice of Medicinal Chemistry

Sous la direction de Camille Wermuth. Academic Press, 1998.

Comment concevoir une molécule biologiquement active dont on pourra faire ensuite un médicament ? C'est la question qu'examine Camille Wermuth et ses collègues dans ce traité de chimie médicinale.

Cette discipline, pierre angulaire de la créativité pharmaceutique, est pratiquée le plus souvent par des chimistes issus des facultés des sciences ou des Grandes Écoles, où l'enseignement de la chimie organique est focalisé sur la réactivité des molécules et sur les grandes méthodes de synthèse ; cet enseignement, essen-

tiel pour la confection des molécules, ne permet toutefois pas de concevoir une molécule «active», de l'adapter à la cible biologique visée, de comprendre son mécanisme d'action, d'optimiser son activité ou de lui éviter une destruction immédiate, après son administration à un être vivant.

L'ouvrage s'efforce de présenter, de façon logique et pédagogique, les points essentiels de la discipline : fonctionnement des récepteurs et des systèmes enzymatiques, influence des paramètres physico-chimiques (polarité, hydrophobicité, structure tridimensionnelle) sur la reconnaissance moléculaire, le métabolisme ou la toxicité. L'ordre utilisé est le suivant : la définition de la chimie médicinale est suivie d'une présentation des cibles des médicaments et des stratégies de découverte des précurseurs actifs ; puis on examine l'influence des paramètres physico-chimiques dans l'établissement des relations qualitatives et quantitatives entre les structures et les activités, on envisage la modélisation des molécules dans leur cible, les études d'optimisation de l'activité, la biodisponibilité des médicaments et les méthodes de vectorisation. Chaque partie est autonome.

Pour présenter les objectifs de la chimie médicinale, les auteurs relatent d'abord l'évolution moléculaire du médicament. L'histoire de la découverte de l'aspirine, qui est donnée dans le livre, est exemplaire et instructive : quand les chimistes ont analysé l'écorce de saule, qui était utilisée comme antipyrétique par la médecine d'antan, ils ont effectivement trouvé un composé actif, l'acide salicylique, qui a ensuite été modifié en acide acétylsalicylique, le composé actif de l'aspirine. Cette histoire est l'occasion de rappeler la liaison fréquente du hasard et de l'observation dans la découverte scientifique.

Les auteurs examinent ensuite le mécanisme d'action des médicaments, montrant comment ces molécules exercent leurs effets pharmacologiques par leur liaison à des molécules nommées récepteurs présents dans divers tissus de l'organisme. On peut regretter l'absence de développement sur les mécanismes d'inhibition des enzymes. En revanche, la présentation, à ce stade, de notions sur la biodisponibilité des molécules sera très profitable au chercheur débutant.

La deuxième partie de l'ouvrage traite de la découverte des composés précurseurs des principes actifs. L'auteur montre

que les approches sont variées et que l'empirisme ne doit pas être rejeté : n'est-ce pas ainsi que fut découvert l'activateur des canaux potassiques, le cromolakin ? Toutefois l'analyse des produits naturels ou des approches modernes, telle la chimie combinatoire, qui engendre une foule de composés que l'on trie ensuite, sont les méthodes modernes que le chimiste doit connaître et pratiquer.

Les principes des relations entre la structure et l'activité biologique des molécules sont abordés dans la troisième partie : connaissant un principe actif, on cherchera à le modifier afin d'engendrer des séries homologues qui pourront faire des composés aux propriétés pharmacologiques supérieures à celles de la «tête de série». Un chapitre entier est consacré à un concept essentiel : le bio-isotérisme qui permet de comprendre comment des molécules apparemment différentes sont reconnues semblables par un récepteur ou par une enzyme). Le chapitre suivant étudie l'influence de l'introduction ou de la suppression des cycles dans les molécules biologiques : de nombreux exemples de simplification de molécules complexes ou d'introduction de contraintes stériques, par cyclisation des molécules actives flexibles, sont présentés.

La quatrième partie de l'ouvrage traite de l'aspect quantitatif des relations entre la structure d'une molécule et son activité biologique. Après un bilan complet des influences de divers groupes chimiques sur l'activité pharmacologique, on examine les aspects moléculaires et thermodynamiques de l'interaction molécule-récepteur. Il est dommage que, dans cette partie, l'aspect plus classique des relations quantitatives entre la structure et l'activité biologique (QSAR) n'ait pas été développé davantage. Le débutant aura du mal à y trouver les notions indispensables à la compréhension de ces approches.

Puis les auteurs introduisent les notions de relations structurales entre une molécule active et sa cible. Les points fondamentaux de la conception moléculaire y sont présentés : conformation active, influence de la stéréochimie et de la configuration de la molécule sur l'activité biologique, rôle des contraintes stériques sur le profil pharmacologique des molécules. Ces notions sont traitées dans cette partie de l'ouvrage que l'utilisation de la modélisation moléculaire est traitée. Ces chapitres amènent le lecteur à la compréhension du rôle essentiel des structures tridimensionnelles des protéines (et de leurs récepteurs) sur l'activité biologique et des informations qui peuvent en être déduites pour la conception de nouvelles molécules.

La dernière partie de l'ouvrage est consacrée au métabolisme des molécules,

POUR LA SCIENCE

8, rue Férou 75278 PARIS CEDEX 06
Tél. : 01-55-42-84-00
<http://www.pourlascience.com>

POUR LA SCIENCE Directeur de la rédaction : Philippe Boulanger. Hervé This (Rédacteur en chef), Françoise Ciotti (Rédactrice en chef adjointe), Bénédicte Lecerq (Rédactrice en chef adjointe), Luc Allemand, Yann Esnault, Philippe Pajot, Loïc Mangin (Rédacteurs). Secrétariat de rédaction : Annie Tacquet, Pascale Thiollier, Céline Lapert. Direction Marketing et Publicité : Henri Gibelin, assisté de Séverine Merviel et Christelle Dumas. Direction financière : Pierre Lecomte, assisté de Anne Gusdorf. Fabrication : Jérôme Jalabert, assisté de Camille Laporte. Directeur de la publication et Gérant : Olivier Brossollet.

Ont également collaboré à ce numéro : Bruno Blondel, François Gadet, Daniel Collobert, Jean-Yves Crochet, Bettina Debù, Paul Decaix, Évelyne Host-Platret, Marie-Thérèse Landousy, Philippe Machellet, Valérie Martin-Rolland, Claude Olivier, Bruno Péault, Christophe Pichon, Thomas Pornin, Serge Vaudenay.

SCIENTIFIC AMERICAN Editor : John Rennie. Board of editors : Michelle Press, Mark Alpert, Timothy Beardsley, Carol Ezzell, Marguerite Holloway, Wayt Gibbs, Alden Jayashii, Steve Mirsky, Madhusree Mukerjee, George Musser, Sasha Nemecek, Ricki Rusting, Sara Simpson, Gary Stix, Paul Wallich, Philip Yam, Glenn Zorpette. President and Chief Executive Officer : Joachim Rosler. Chairman : John Hanley. Co-Chairman : Rolf Grisebach. Vice-président : Frances Newburg.

PUBLICITÉ France

Chef de Publicité : Susan Mackie, assistée de Anne-Claire Ternois, 8 rue Férou 75278 Paris Cedex 06
Tél. : 01 55 42 84 28.
Téléc. : LIBEL N 202978F.
Télécopieur : 01 43 25 18 29

Étranger : Kate Dobson, 415 Madison Avenue, New York, N.Y. 10017 - Tél. (212) 754.02.62

SERVICE ABONNEMENTS

Ginette Grémion : 01 55 42 84 04.

SERVICE DE VENTE RÉSEAU NMPP

Henri Gibelin

DIFFUSION DE LA BIBLIOTHÈQUE POUR LA SCIENCE

Canada : Module - 233, avenue Dunbar Mont-Royal, Québec, H3P 2H2 Canada

Suisse : Serolis - 5, rue des Chaudronniers - 15 Postale 3663 - CH 01211 Genève

Autres pays : Éditions Belin - B.P. 205, 75264 Paris Cedex 05.

Toutes demandes d'autorisation de reproduire, pour le public français ou francophone, les textes, les photos, les dessins ou les documents contenus dans la revue «Pour la Science», dans la revue «Scientific American», dans les livres édités par «Pour la Science» doivent être adressées par écrit à «Pour la Science S.A.R.L.», 8, rue Férou, 75278 Paris Cedex 06.

© Pour la Science S.A.R.L.

Tous droits de reproduction, de traduction, d'adaptation et de représentation réservés pour tous les pays. La marque et le nom commercial «Scientific American» sont la propriété de Scientific American, Inc. Licence accordée à «Pour la Science S.A.R.L.»

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement la présente revue sans autorisation de l'éditeur ou du Centre Français d'exploitation du droit de Copie (3, rue Hautefeuille - 75006 Paris).

Nos lecteurs trouveront dans ce numéro des bulletins d'abonnement en pages 18A, 18B, 98A et 98B.

à leur transformation, à leur élimination et aux moyens utilisés pour en améliorer la biodisponibilité. Ces chapitres sont particulièrement importants pour le chimiste, car la mise au point des médicaments est fréquemment entravée par une mauvaise biodisponibilité ou par des effets toxiques des molécules actives. Ces inconvénients, pris en compte par le concepteur des molécules, peuvent être parfois évités par une bonne connaissance du métabolisme et des diverses transformations chimiques qui en résultent.

L'ouvrage se termine par une présentation des diverses étapes de la mise au point d'une nouvelle molécule et des aspects réglementaires rencontrés lors de sa commercialisation. Comme le souhaitait son auteur principal, le livre remplit parfaitement les objectifs qu'il s'était fixés : il montre bien à de jeunes scientifiques comment se pratique la chimie médicinale, il explique bien pourquoi cette pratique est pluridisciplinaire et pourquoi des règles empiriques cotoient nécessairement les outils modernes de la conceptualisation.

Michel LANGLOIS

Météorologie

Les eaux du ciel

Robert Kandel. Hachette Littérature, 1998.

La dernière phrase de ce livre en donne parfaitement l'esprit : après avoir invité le lecteur à boire un verre de cette eau dont il vient de retracer l'histoire, Robert Kandel écrit : «Vous préférez le vin ? À l'eau évaporée de l'Atlantique et retombée sur les vignes du Bordelais, la nature et le vigneron ont ajouté du soleil, du CO₂, des poignées d'autres éléments, d'autres poussières d'étoiles. À votre santé !»

Le livre tout entier invite le lecteur à jeter un regard différent sur le monde qui nous entoure, à la lumière de recherches scientifiques parfois récentes, souvent anciennes. Le cours complexe des «eaux du ciel» nous conduit dans les lieux les plus variés de notre planète, voire du Système solaire, des antilles de la Terre au milieu des grandes neiges, en passant par les nuages. R. Kandel décrit aussi les enjeux de l'eau, source de vie, objet d'inquiétudes et de conflits.

L'ouvrage se caractérise par la combinaison d'un sérieux et d'une précision constantes, et le souci de toujours garder le ton d'un récit ou d'une causerie ;

on pourrait presque parler d'impressions de voyage. Je pense d'ailleurs que ce texte, qui aborde une grande variété de phénomènes, impossible à résumer ici, s'accorde parfaitement d'une lecture au hasard.

Un point me paraît important à signaler : Les *Eaux du ciel* ne sont ni un livre de réflexion sur la science, ni un livre de présentation des méthodes scientifiques. Il ne contient pas de schémas, pas d'équations, peu de chiffres, mais beaucoup de faits et d'explications. La vulgarisation scientifique de ce genre me paraît importante.

Depuis le début du siècle, la durée des études nécessaires pour appréhender un domaine de recherche s'est considérablement allongée, avec le perfectionnement des méthodes mises en jeu. Dans le même temps, la science est devenue un enjeu social de plus en plus important. Deux des problèmes qu'aborde R. Kandel, l'effet de serre et les déchets nucléaires, sont exemplaires à cet égard. Leurs conséquences sont trop fortes, les incertitudes scientifiques trop nombreuses pour que leur discussion demeure confinée dans le monde de la science ou de la technique : les décisions doivent faire l'objet de débats démocratiques.

Ce qui illustre clairement le livre de R. Kandel (et les textes de quelques autres apparus dans ce numéro, malgré tout dans un domaine), c'est que l'appareil mathématique et technique qui est nécessaire à la recherche scientifique n'est, au contraire, pas indispensable pour en exposer les résultats. Il fait preuve à cet égard d'une pédagogie souvent originale : l'évocation de deux enfants sur une balançoire, au Parc Montsouris, donne une vision finalement assez exacte de l'oscillation El Niño/La Niña.

L'auteur montre aussi – c'est peut-être le plus important – que cette vulgarisation peut se faire sans concessions ni simplification réductrices des faits. Sans doute un effort est-il demandé parfois au lecteur, mais le livre est abordable par tous, et il fournira à tous une occasion d'aborder les problèmes de l'environnement global sans connaissances préalables, dans le respect de leur complexité. Aux scientifiques, il apportera une certaine distance du regard sur leur discipline, distance qui leur manque parfois lorsqu'elle est, ô combien, stimulante.

Hervé LE TREUT

La liste de tous les livres reçus en service de presse par la rédaction de Pour la Science est donnée sur notre site Internet, à l'adresse :

<http://www.pourlascience.com>