

LES KANGOUROUS TUEURS • LES CELLULES SOUCHES HUMAINES • LE SATELLITE ISO

Pour la Science

■ POUR LA

SCIENCE

Juin 1999

édition française de

SCIENTIFIC
AMERICAN

Dossier :
*La sécurité
sur l'Internet*

Canada : \$ 8,75

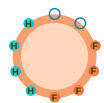
Les raz-de-marée



BLOC-NOTES

de Didier Nordon

5



JEU-CONCOURS

Dîner de mathématiciens

par Pierre Tougne

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 Diane Proudfoot

12



SCIENCE ET GASTRONOMIE

Arômes ou réactions ?

par Hervé This

16



PERSPECTIVES SCIENTIFIQUES

■ L'astronome astrologue ■ L'amour est aveugle

■ Un très vieux atelier ■ Turbulence et transition

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

■ Cartes d'extinction ■ Calcul verbal

20



IDÉES DE PHYSIQUE

Le gravidyne

par Roland Lehoucq

100



LOGIQUE ET CALCUL

Premiers jumeaux frères ennemis?

par Jean-Paul Delahaye

102



VISIONS MATHÉMATIQUES

Tours, tortillements, topologie et téléphone

par Ian Stewart

108



ANALYSES DE LIVRES

■ Les Orchidées de France, Belgique et Luxembourg, ouvrage collectif de la Société française d'Orchidophilie, sous la direction de Marcel Bourmérias

■ 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

110

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.

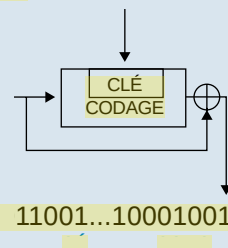


Cryptographie et réseau

38

par Philip Zimmermann

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

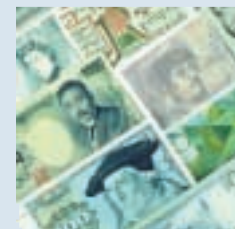


Le paiement sur l'Internet

45

par Octavian Ureche et Réjean Plamondon

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

par Roger Pedersen

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



58

Les tsunamis

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.



64

Le syndrome postpolio

par 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.



76

Les kangourous carnivores

par Stephen Wroe

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

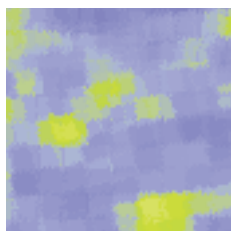


82

Le ciel infrarouge vu de l'espace

par A. Abergel, F. Boulanger, G. Lagache, E. Dartois 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.



82

La grand'peur de l'Internet

Trissotin :

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

Philaminte :

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 nombres 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 Beuzamy 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