aura été crypté avec lui ne sera-t-il pas alors accessible à chacun facilement?

Citons encore le cas du *RSA for paranoids* proposé par A. Shamir (le «S» du RSA) en 1995. Il s'agit d'une variante du RSA, destinée à rassurer les utilisateurs inquiets du RSA classique en leur permettant d'utiliser, sans trop augmenter les coûts de codage, des nombres *n* plus longs. Trois ans après, ce prétendu renforcement du RSA était cassé par H. Guilbert, D. Gupta, A. Odlyzko et J.-J. Quisquater, qui en identifiaient de graves points faibles. Ainsi, l'un des inventeurs du RSA, croyant renforcer sa méthode dans le but de satisfaire les paranoïaques, a renforcé leurs craintes. Si nous souhaitons protéger des données pour une longue période de temps, soyons conscients que tout s'appuie, en cryptographie mathématique, sur un état de l'art qui peut changer rapidement et dont la réalité est peut-être déjà totalement autre que celle présentée au public.

Le grand nombre de systèmes nouveaux inventés chaque année et qu'on exhibe dans le but de calmer les inquiets («de toutes les façons, si tel système est cassé vous pourrez toujours utiliser celui-là») ne résout en rien le problème, qui est de disposer d'UN système prouvé robuste. Rien ne ressemble plus à un système cryptographique solide qu'un système cryptographique faible, et aujourd'hui personne ne dispose vraiment des moyens de garantir sérieusement aucun des systèmes largement utilisés.

## ALTERNATIVE QUANTIQUE?

L'usage de la cryptographie quantique, dont la garantie ne repose pas sur des conjectures mathématiques, mais sur des principes de physique fondamentale, résoudra peut-être ce problème. La maturité de cette technique la rend utilisable aujourd'hui pour les applications où l'émetteur et le récepteur ne sont pas éloignés de plus de cent kilomètres.

Un autre résultat lié aussi à la mécanique quantique contribue à rendre encore plus méfiant vis-à-vis de la cryptographie mathématique. Peter Shor a montré en 1994 qu'avec un ordinateur quantique on peut factoriser efficacement des nombres entiers. Si l'on réussit à construire de telles machines, tout un pan de la cryptographie mathématique sera définitivement compromis. Les ordinateurs quantiques aujourd'hui sont de simples fictions théoriques dont la difficile mise au point devrait demander des années (si elle se révèle possible) ; cependant, là encore, l'avance possible de certains services secrets n'est pas à exclure et, si elle est réellement sensible, alors il se peut que pour eux la factorisation des clefs de 1 024 bits ou de 2 048 bits du RSA soit devenue un jeu d'enfants. Gilles Brassard, chercheur canadien renommé, passé de la cryptographie mathématique à la recherche sur les techniques quantiques, remarque que la mécanique quantique non seulement fait percevoir la fragilité fondamentale de la cryptographie mathématique, mais propose une solution pour échapper aux incertitudes dont elle ne réussit pas à se libérer.

### 6.LE RECORD DE FACTORISATION DU 22 AOÛT 1999

Le travail nécessaire aux grandes factorisations est complexe : voici quelques détails sur le calcul mené pour venir à bout du RSA-155. Le 22 août 1999, une équipe de l'Institut national de recherche en mathématiques et en science informatique d'Amsterdam annonçait avoir cassé la clef numérique de 512 bits (155 chiffres décimaux), problème connu sous le nom du RSA-155. Le résultat trouvé tient en quelques lignes ; c'est la factorisation d'un nombre de 155 chiffres en deux nombres premiers de 78 chiffres :

109417386415705274218097073220403576120037329454492059909138421314763499842889347847179972578912673324976257528997818337970765372440271467435315933543338 97

=102639592829741105772054196573991675900716567808038066803341933521790711307779 × 106603488380168454820927220360012878679207958575989291522270608237193062808643

Trois cents ordinateurs divers (stations de travail et PC) ont travaillé à ce résultat cumulant un total de calcul évalué à 8 000 Mips année (1 Mips = un million d'instructions par seconde). Le déroulement des opérations s'est étalé sur une période de trois mois et demi. La primalité des facteurs a été évaluée par deux méthodes différentes. L'algorithme utilisé est le GNFS *(General Number Field Sieve)*, qui déjà avait permis de battre le précédent record de factorisation, le RSA-140, en février 1999.

Une légère amélioration de la méthode utilisée pour le RSA-140 a été utilisée. Si la méthode du RSA-140 avait été reprise sans modification, 14 000 Mips années auraient été nécessaires. Ainsi, en six mois, les progrès théoriques ont économisé 40 pour cent du calcul. En y ajoutant les progrès technologiques des microprocesseurs et la capacité accrue des réseaux pour faire coopérer des ordinateurs, la puissance a été doublée en six mois.

Le travail s'est déroulé en une série complexe de phases nécessitant des ordinateurs et des combinaisons d'ordinateurs variées. La première phase a consisté à rechercher un bon jeu de paramètres pour la méthode. On évalue à 100 Mips année la quantité de calculs faite pour cette phase, qui a duré neuf semaines en utilisant une seule machine (de type 250 Mhz *GI Origin* 2000). Cette partie du calcul ne se laisse pas distribuer sur un réseau.

La seconde phase, qui a été distribuée sur un réseau de 300 machines réparties dans le monde entier, est aussi la plus coûteuse en calcul. Elle a fourni des relations qui sont au cœur de la méthode. Un total de 124 millions de relations a ainsi été engendré, dont 39 millions apparaissaient en double (à cause de la méthode de calcul distribué).

Le tri des relations et la préparation de la matrice du système linéaire à résoudre ont été réalisés au CWI, ce qui a demandé un mois de travail. La matrice résultante comportait 6 699 191 lignes et 6 711 336 colonnes.

La résolution du système d'équations a alors demandé 224 heures et 2 gigaoctets de mémoire centrale à un ordinateur *Cray C916*, un ordinateur vectoriel destiné à mener de très gros calculs (par exemple en météorologie), calculs impossibles à répartir sur un réseau de machines moyennes.


**D BONEH, *Twenty Years of Attacks on the RSA Cryptosystem,* in *Notice of the AMS* (American Mathematical Society), pp. 203-213, février 1999.**

**D. BONEH et R. VENKATESAN, *Breaking RSA May Be Easier Than Factoring,* Eurocrypt 1998, LNCS 1403, Springer-Verlag, pp. 59-71.**

**P. C. KOCHER, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and other Systems,* Crypto 1996, LNCS 1109, Springer-Verlag, pp. 104-113.**

**A.M. ODLYZKO, *The Rise and Fall of Knapsack Cryptosystems,* ATT Bell Laboratories, Murray Hill, 1990.**

**B. SCHNEIER, *Cryptographie appliquée,* Thomson Publishing France, Paris, 1995.**

**J. STERN, *La science du secret,* Odile Jacob, Paris, 1998.**

# Botanique

## Guide de l'amateur de cactus

Pierre-Louis Fröling. Éditions Belin, 1998.

Dans tout western de la grande époque, un personnage muet, géant, à la rigide et menaçante silhouette en chandelier, se dresse au moment décisif : il s'agit, bien entendu, d'un *Carnegia* multiséculaire, auprès duquel les héros du film trouvent un précaire repos, ignorant leurs poursuivants tapis derrière l'entrelacs d'*Opuntia* hérissés d'épines... Les deux plantes citées, dites grasses («succulentes» est le terme approprié), cactées dans le langage courant, peuplent, avec beaucoup d'autres «épineux» les semi-déserts du Sud-Ouest des États-Unis, contribuant à l'étrange beauté d'un paysage végétal sans équivalent dans le monde. Mais sait-on que certaines cactées fréquentent les forêts humides d'Amérique centrale ? Que d'autres vivent à des altitudes atteignant 6 000 mètres, dans les Andes péruviennes ?

Ce superbe ouvrage nous convie à beaucoup d'autres découvertes, à propos de l'une des deux grandes familles végétales (nom officiel : cactacées, de *cactos*, qui signifie «épineux»), famille relativement récente, à l'échelle de l'évolution, puisque quasi exclusivement américaine à l'état spontané (le seul genre *Rhipsalis*, ayant tardivement gagné l'Afrique, constituant une remarquable exception). Parmi les plantes suscitant dans le public le plus d'intérêt et de curiosité, les cactées sont en tête, avec les orchidées et les plantes carnivores. En témoigne le nombre de visiteurs du Jardin exotique de Monaco, fascinés par la fragile splendeur de fleurs surgies d'organismes redoutablement armés, dont l'étrange géométrie pourrait laisser douter de leur nature végétale.

Parmi les nombreuses espèces de cactées (environ 1 400, nous dit Aline Raynal-Roques, dans une préface inspirée), l'auteur a retenu les «cent plus belles», choix parfaitement justifié au vu des splendides photographies qui présentent chacune d'entre elles (souvent par plusieurs images de grand format : la plante dans son milieu, ses fleurs...). Elles sont l'objet d'une monographie parfaitement claire, où se succèdent l'étymologie des noms scientifiques de genre et d'espèce (éventuellement les synonymes latins, les noms vernaculaires), son habitat, sa répartition géographique, sa morphologie et sa biologie florale, ses conditions de culture (avec un tableau résumé très pédagogique), les espèces voisines... Outre les floraisons présentées, spectaculaires par leurs dimensions ou leurs coloris délicats, souvent éphémères (chez la reine de nuit, *Selenicereus grandiflorus*, la floraison coïncide avec la période nocturne), l'ouvrage nous révèle l'étonnante diversité des formes que ces plantes ont su réaliser à partir de modèles simples (cylindre, sphère, ballon de rugby, raquette…). Malgré leur morphologie typique des régions sèches, certaines croissent dans les forêts tropicales humides, parfois en épiphytes, comme des *Epiphyllum*, dont certains supportent les climats pluvieux.

Après l'éblouissante partie monographique, d'autres chapitres sont d'une grande richesse d'information et n'intéresseront pas seulement les amateurs de cactées. Certains, didactiques et parfaitement illustrés, traitent de la culture, des maladies et des multiples adaptations morphologiques, anatomiques et physiologiques des cactées liées à leurs milieux de vie. À côté des procédés de reproduction, sexuée et végétative, relativement classiques, l'auteur présente avec soin l'une des originalités de ces plantes : leur étonnante possibilité de xénogreffes. Celles-ci, dont les techniques sont précisées, peuvent même être pratiquées entre certaines cactacées et des didiéracées (une étrange famille endémique des milieux semi-arides de Madagascar), cas sans doute unique qui révèle les affinités systématiques entre les deux familles.

Notons aussi la confrontation de la taxinomie des cactées (dont les étapes, de Linné à aujourd'hui, sont précisées) avec la classification «indienne» (précolombienne), illustrée notamment de dessins tirés du célèbre *Codex Mendoza*, l'analyse de l'origine géographique, des mécanismes de l'évolution, de la répartition des cactées sur plus de 10 000 kilomètres en latitude (des montagnes de Colombie britannique, où *Opuntia polyacantha* supporte des températures aussi basses que –30 °C, jusqu'à la Patagonie). À côté de données sur les utilisations actuelles de cactus (notamment l'élevage de la cochenille), l'auteur a pris visiblement plaisir à rassembler documents historiques et anecdotes folkloriques sur les multiples pratiques religieuses ou magiques d'Amérique du Sud, et dont on retrouve l'écho dans les tentatives actuelles de démontrer les facultés sensorielles de ces plantes énigmatiques : une cactée (vendue en France) serait particulièrement apte à protéger les micro-ordinateurs de toute panne informatique ! En revanche, les espèces rares de cactées ne savent pas se protéger elles-mêmes de l'avidité mercantile des collecteurs. Outre un utile rappel des règles déontologiques que tout amateur doit avoir à l'esprit, l'auteur précise les mesures légales permettant la survie des plus menacées : création de réserves naturelles, lourdes sanctions contre les pillards, liste des cactées visées, au titre du commerce international, par la CITES, convention ratifiée par 130 nations.

Par le nombre considérable d'informations qu'il contient, ce livre dépasse largement ce que pourrait suggérer son titre. Il ne s'adresse pas seulement au collectionneur de cactées, mais aussi

© Solichon

***Astrophytum myriostigma* pousse à plus de 2 000 mètres d'altitude, sur le sol calcaire des hauts plateaux du Mexique.**