apparent soit faussé, en opérant des calculs supplémentaires inutiles une fois le codage réalisé, avant d'envoyer l'information que le codage est terminé.

ON NE S'IMPROVISE PAS CRYPTOGRAPHE

De nombreuses erreurs dans la gestion imprudente ou maladroite des clefs sont aussi à l'origine de décryptages inopinés des messages considérés inviolables, car obtenus avec RSA. Une prudence à tous les niveaux est indispensable pour en arriver à des systèmes fiables. Dans un article paru en 1999, Dan Boneh, qui est le grand spécialiste des attaques du RSA proposait cette conclusion rassurante : «En ce moment, il apparaît que l'on peut avoir confiance dans la sécurité que procure le RSA au monde numérique.» Bruce Schneier, un autre spécialiste international de la cryptographie très préoccupé des réalisations opérationnelles, insiste sur le fait que la plupart des systèmes de cryptographie qu'on a réussi à casser l'ont été, non par l'attaque réussie du noyau mathématique du système, mais à cause de faiblesses dans la mise en œuvre : mauvaise génération des clefs, mots de passe mal choisis ou mal protégés, contournement possible de l'algorithme mathématique, etc.

L'idée défendue que le noyau mathématique du RSA est inviolable est seulement une conclusion expérimentale tirée de l'échec des tentatives connues d'attaques du RSA (lorsqu'on l'utilise en respectant les consignes formulées par les spécialistes… dont la liste s'allonge chaque année). Cette conclusion n'interdit pas que le risque théorique lié au RSA puisse être jugé grand, puisqu'on n'a ni réussi à montrer que la factorisation est difficile (aucun espoir n'existe à court terme qu'on y arrive), ni même réussi à montrer que le RSA est aussi difficile que la factorisation.

À l'évidence, si une agence de renseignements a découvert quelque chose concernant la factorisation ou s'appliquant directement au RSA sans passer par la factorisation, elle ne rendra pas publique sa découverte et, au contraire, fera tout pour la maintenir secrète le plus longtemps possible. Dire cela n'est pas faire preuve d'une méfiance maladive, mais du simple bon sens. La tranquille assurance exprimée par les spécialistes à propos de la sécurité du RSA apparaît incompréhensible, et parfois même assez louche.

Dix fois, dans l'histoire des services d'espionnage, un système de codage a été considéré cent pour cent sûr et inviolable par ceux qui l'utilisaient, alors qu'au même moment un service ennemi ayant percé le secret du système lisait tranquillement tous les messages qui tombaient entre ses mains. Cela s'est produit pendant la Première Guerre mondiale : les services français décodaient chaque nuit les messages destinés aux U-boot tapis au fond de la Méditerranée, ce qui permettait de modifier avant l'aube les programmes de navigation des bateaux menacés. À nouveau, pendant la Seconde Guerre mondiale, cela s'est produit avec la fameuse affaire de la machine *Enigma*, où s'illustra Alan Turing. Signalons aussi l'extraordinaire secret qui a entouré cette aventure impliquant les centaines de personnes qui ont travaillé au Bletchley Park, près de Londres, qui toutes sont restées muettes pendant trente ans : le sens patriotique est une motivation suffisante pour faire taire même le mathématicien le plus soucieux du partage de ses découvertes. Il me semble que, si un mathématicien canadien (même s'il est universitaire) découvre quelque chose d'important sur la factorisation, il le gardera pour les militaires canadiens, de même qu'un mathématicien français réservera ses théorèmes cryptographiques cruciaux pour les militaires français, etc.

Pourquoi donc, alors que des moyens considérables sont consacrés à la cryptanalyse – et donc à toutes les mathématiques et techniques qui y sont liées – par les agences spécialisées de renseignements puissantes et fortunées, ne pas envisager sérieusement, qu'ignorée des circuits de la recherche universitaire (et provenant peut-être d'un universitaire patriote), une découverte fondamentale faisant tomber le RSA ait été faite et reste cachée?

Même si l'on n'est pas paranoïaque, en l'absence de résultats mathématiques établissant la sécurité du RSA, il est sage de ne pas trop lui faire confiance. Réalise-t-on, quand on utilise la méthode de cryptage à deux étages évoquée plus haut (RSA pour communiquer une clef, puis algorithme symétrique), que si un seul des deux étages est percé c'est tout le système qui coule? Comment ne pas penser à de la désinformation quand on lit, en contradiction avec tout bon sens, que le système à deux étages est d'autant plus solide qu'il utilise deux méthodes cryptographiques !

A. M. Odlyzko a publié un bilan sur le cryptosystème à double clef de Merkle et Hellman fondé sur le problème du sac à dos (un problème combinatoire de rangement). Grâce à certaines propriétés mathématiques le reliant à d'autres problèmes assez bien compris, ce cryptosystème fut considéré un temps comme plus prometteur que le RSA. Malheureusement, il fut cassé, et les variantes qui ont été proposées aujourd'hui de ce système se sont révélées pour l'essentiel aussi fragiles que la version originale, tant et si bien que du système le plus prometteur d'il y a 15 ans il ne reste rien aujourd'hui. N'en sera-t-il pas de même pour le RSA dans 15 ans, et tout ce qui

4. LE CALCUL DE L'EXPONENTIATION RAPIDE

Dans la mise en œuvre aussi bien des algorithmes probabilistes pour engendrer des nombres premiers que pour l'implémentation du RSA, on a besoin de calculer rapidement A^e mod n. Voici une méthode (dont le principe général est emprunté à la multiplication égyptienne) qui permet ce calcul.

Calcul de A^e mod n

- partir du triplet $(A, e, 1) = (P, J, R)$ puis :
- si J est pair, passer à $(P^2 \bmod n, J/2, R \bmod n)$
- si J est impair, passer à $(P^2 \bmod n, (J-1)/2, R \times P \bmod n)$
- s'arrêter si $J = 1$, le résultat est $R = P \bmod n$

Exemple :

$A^{13} \bmod n \longrightarrow (A,13,1) \longrightarrow (A^2 \bmod n, 6, A) \longrightarrow (A^4 \bmod n, 3, A) \longrightarrow (A^8 \bmod n, 1, A^5) \longrightarrow R = A^{13} \bmod n$. Avec $n = 5$ et $A = 2$:

$213 \bmod 5 \longrightarrow (2,13,1) \longrightarrow (4, 6, 2) \longrightarrow (1, 3, 2) \longrightarrow (1, 1, 2) \longrightarrow R = 2$

5. EXEMPLE NUMÉRIQUE SIMPLIFIÉ DE CODAGE RSA

$p = 47$, $q = 71$, $n = pq = 3337$, $(p-1)(q-1) = 3220$, $e = 79$, $d = 1019$

On vérifie que $ed = 80501 = 25 \times 3220 + 1 = 1 \bmod 3220$

Prenons un message préalablement transformé en un nombre :

$m = 6882326879666683$

On découpe m : $m_1 = 688$ $m_2 = 232$ $m_3 = 687$ $m_4 = 966$ $m_5 = 668$ $m_6 = 3$

Le premier bloc est chiffré par le nombre $c_1 = 688^{79} \bmod 3337 = 1570$;

de même : $c_2 = 2756$ $c_3 = 2091$ $c_4 = 2276$ $c_5 = 2423$ $c_6 = 158$.

Le déchiffrement du message se fait en calculant :

$c_1 = 1570^{1019} \bmod 3337 = 688$, etc.

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.

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 :

109417386415705274218097073220403576120037329454492059909138
421314763499842889347847179972578912673324976257528997818337
970765372440271467435315933543338 97
=102639592829741105772054196573991675900716567808038066803341
933521790711307779 × 106603488380168454820927220360012878 67
920795857598929152227060823719306280864 3

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.

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.

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.