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.