# 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, mais les enveloppes cachent le contenu des messages. 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, très efficaces, résistent à toute tentative de «cassage».

## 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», 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 au point hors de la communauté militaire. Les 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. Ce procédé, dit asymétrique, repose sur un couple de clés complémentaires. 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 déchiffrer. Ainsi, l'une des clés complémentaires (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 utilise les logarithmes discrets, c'est-à-dire que l'on calcule des valeurs du type $g^x$ 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 cette division. L'opération inverse est un problème redoutable : même si l'on connaît les valeurs numériques de $g$, de $p$ et de $g^x$ modulo $p$, il est impossible, en pratique, de retrouver $x$ (voir *Les mathématiques de la cryptographie à clef révélée*, 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 41)*, puis il chiffre ce condensé 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.**