

toferrine et du lysozyme. Des molécules de ces trois types sont plus abondantes dans l'urine de nourrissons allaités que dans celle d'enfants nourris au lait maternisé. Pourtant les enfants allaités ne peuvent absorber ces molécules à partir du lait maternel ; aussi pense-t-on que ces molécules sont produites par les muqueuses des voies urinaires et que l'allaitement maternel induit une immunité locale de ces voies.

Cette hypothèse semble confirmée par des études récentes : on a observé que, chez le nourrisson, le risque d'infections urinaires est réduit. Un facteur inconnu, présent dans le lait maternel semble, notamment, faire produire plus de fibronectine à l'organisme des enfants allaités qu'à celui des enfants nourris au biberon. Au total, le lait maternel est donc un liquide tout à fait remarquable : il nourrit, et il protège les enfants jusqu'à ce que ceux-ci soient capables de se protéger tout seuls.

Jack NEWMAN a fondé plusieurs cliniques pédiatriques à Toronto. Il est professeur de pédiatrie à l'Université de Toronto.

H.B. SLADE et S.A. SCHWARTZ, *Mucosal Immunity : The Immunology of Breast Milk*, in *Journal of Allergy and Clinical Immunology*, vol. 80, n° 3, pp. 348-356, septembre 1987.

Immunology of Milk and the Neonate, sous la direction de J. Mestecky et al., Plenum Press, 1991.

Allan S. CUNNINGHAM, *Breastfeeding and Health in the 1980's : A Global Epidemiologic Review*, in *Journal of Pediatrics*, vol. 118, n° 5, pp. 659-666, mai 1991.

A.S. GOLDMAN, *The Immune System of Human Milk : Antimicrobial, Antiinflammatory and Immunomodulating Properties*, in *Pediatric Infectious Disease Journal*, vol. 12, n° 8, pp. 664-671, août 1993.

Ruth A. LAWRENCE, *Host-Resistance Factors and Immunologic Significance of Human Milk*, in *Breastfeeding : A Guide for the Medical Profession*, Mosby Year Book, 1994.

Bernard THIS, *Neuf mois dans la vie d'un père*, InterÉditions, 1995.

Jean-François BACH, *Traité d'immunologie*, Éditions Flammarion.

J. BROSTOFF, G.K. SCADDING, D. MALE et I.M. ROITT, *Immunologie clinique*. Éditions de Boeck-Université.

La confidentialité des communications

THOMAS BETH

Un nouveau protocole cryptographique utilisant des «passeports numériques» assure la sécurité des réseaux informatiques en permettant l'authentification des correspondants.

«Mes chers petits, je vais dans la forêt ; prenez bien garde au loup, car s'il entrerait, il vous dévorerait tout crus. Le vaurien se déguise souvent, mais vous le reconnaîtrez sans peine à sa voix rauque et à ses pattes noires.»

Grimm,

Le loup et les sept chevreux.

La chèvre essaie de protéger ses petits au moyen de ce qu'un expert en sécurité informatique nommerait un protocole de contrôle d'accès : ne laissez entrer que ceux qui possèdent une voix douce et des pattes blanches. Cette méthode est efficace, car elle est fondée sur l'aspect physique des personnes susceptibles d'entrer ; néanmoins, dans le conte, elle est mise en défaut, parce que la quantité d'information utilisée est insuffisante : la distinction entre un loup et une chèvre est aisée si le corps tout entier est observable, mais ici, les chevreux n'ont été programmés que sur la reconnaissance de la voix et de la couleur des pattes...

Les ordinateurs échangent tant d'argent et d'informations précieuses que des pirates de l'informatique essaient de capter leurs messages. Pourtant, ceux qui veulent protéger leurs données sont moins prudents que la chèvre du conte : ils cherchent à distinguer les «bons» des «méchants» en utilisant uniquement des suites de symboles.

La puissance croissante des ordinateurs et l'anonymat offert par les réseaux effraient les gouvernements, qui prévoient une recrudescence des piratages informatiques. De nom-



1. CETTE MONTRE cryptographique fabriquée par la Société autrichienne *Skidata Computer*, contient un émetteur-récepteur ainsi qu'un micro-ordinateur.

breuses nations ont réagi en proposant des remèdes draconiens, qui sont quelquefois pires que le mal. Mes collègues et moi-même pensons avoir trouvé une solution à mi-chemin entre les dangers d'un contrôle étatique absolu et une liberté laissant le champ libre aux abus de toutes sortes.

Toute personne communiquant à l'aide d'ordinateurs requiert un système de sécurité répondant à trois critères : la confidentialité, l'authentification et la confiance. Des actions aussi routinières que de retirer de l'argent d'un distributeur automatique sont fondées sur la confiance. Le système opère alors en sens unique : en demandant un mot de passe secret, la machine s'assure que la personne qui a introduit la carte en est bien le propriétaire légitime, mais celui qui retire de l'argent doit aveuglément faire confiance à la machine

et supposer qu'elle n'est pas corrompue. Bien que ce modèle autoritaire ait été approprié, il est naïf de supposer que les machines qui participent aux transactions actuelles ne sont jamais manipulées.

Tant qu'une même institution assure les communications, on garantit l'authentification et la confidentialité par le principe des protocoles d'échange de clés et de certificats gérés par un serveur central. Le système Kerberos du réseau Athena, à l'Institut de technologie du Massachusetts, utilise ce principe (voir *Réseaux informatiques et sécurité*, par Jeffrey Schiller, *Pour la Science*, janvier 1995).

Il serait absurde d'utiliser la même méthode pour les millions d'utilisateurs du réseau *Internet*. Tout d'abord, il serait impossible de constituer et de gérer un serveur de fichier centralisé qui contiendrait toutes les informations nécessaires aux échanges confidentiels. Ensuite, une telle concentration de données importantes serait une proie des plus tentantes.

En outre, sur un réseau public, les vérifications d'identité à l'aide de mots de passe ne sont pas sûres. Des programmes espions qui enregistrent subrepticement les noms des utilisateurs et leurs mots de passe peuvent en faire un usage ultérieur frauduleux. De tels programmes ont été utilisés dans des dizaines de piratages graves aux États-Unis et en Europe. On ne doit donc pas imposer aux utilisateurs des réseaux de révéler leur mot de passe ou une quelconque caractéristique personnelle qui pourrait être copiée. Idéa-

lement, les programmes d'identification devraient poser des questions afin de vérifier que l'utilisateur possède un secret (un mot de passe, par exemple) sans le révéler.

À l'Université de Karlsruhe, nous avons mis au point un système de sécurité des réseaux nommé SELANE, l'acronyme de *secure local area network*, soit «réseau local sécurisé». Ce nom est aussi une allusion à la déesse grecque de la Lune, Séléné, qui est l'égale dans le ciel de ses deux frères Éos et Hélios, tout comme les deux parties d'une transaction électronique doivent être d'égale importance.

Le système SELANE est utilisable par n'importe quel réseau commercial ou universitaire. Nous avons également créé une carte à puce qui sécurise les opérations nécessaires à chaque utilisateur.

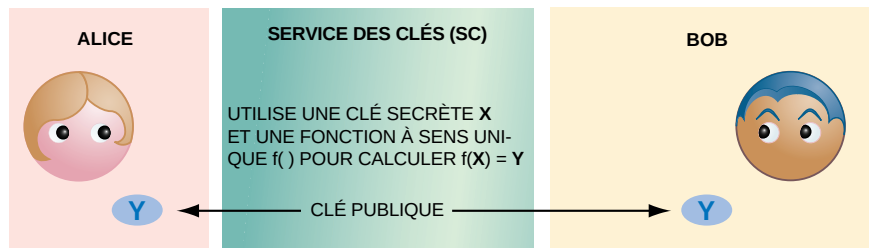
Partager des clés secrètes

La cryptographie moderne considère que les textes représentés par des suites de bits peuvent être interprétés comme des nombres. Le chiffrement n'est alors que l'application d'une fonction mathématique permettant de transformer une chaîne de nombres écrite en clair en une chaîne inintelligible, qui ne peut être lue que par une personne connaissant la fonction et la clé de déchiffrement.

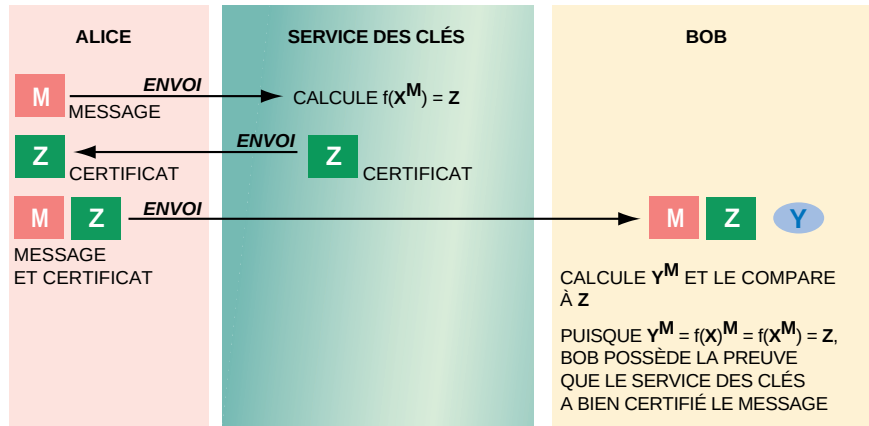
La confidentialité est la première nécessité d'un réseau sécurisé. Comment Alice et Bob (noms génériques donnés par les cryptographes aux deux correspondants d'une communication) peuvent-ils échanger un message confidentiel en utilisant une ligne sur écoute? Au minimum, ils doivent échanger une clé qui servira à chiffrer ou à déchiffrer les messages qui suivront. Vers 1970, à l'Université de Stanford, Martin Hellman, Whitfield Diffie et Ralph Merkle ont conçu une méthode qui permet à Alice et à Bob d'obtenir une même chaîne de bits sans envoyer sur la ligne de communication ni les bits eux-mêmes, ni les informations nécessaires à leur reconstruction (voir l'encadré ci-contre).

Cette méthode est fondée sur l'emploi de «fonctions à sens unique possédant une trappe», que l'on calcule aisément, mais qui sont quasi impossibles à inverser : même si un pirate connaissait le résultat de la transformation d'un nombre par une telle fonction, il ne pourrait retrouver le nombre

DISTRIBUTION D'UNE CLÉ PUBLIQUE



AUTHENTIFICATION DES MESSAGES



2. LES PROTOCOLES d'authentification reposent sur une séquence secrète de bits connue seulement par l'organisme qui les délivre et sur une succession d'exponentielles. Cet organisme ne publie qu'une version chiffrée de sa séquence secrète, mais il donne la possibilité de vérifier que c'est bien lui qui a signé un document donné.

Des fonctions à sens unique pour vaincre les oreilles indiscrettes

Le procédé d'échange de clés de Diffie-Hellman permet à deux correspondants de communiquer de manière sûre, même en utilisant une ligne sur écoute. Cet échange est fondé sur des fonctions à sens unique nommées exponentielles modulaires. Pour appliquer ce procédé à un message, on élève une constante (par exemple, 3) à une puissance représentant le message sous forme numérique, puis on prend le reste de la division par un grand nombre premier. Par exemple, pour chiffrer le nombre 66, on calcule le reste de la division de 3^{66} par 127 (en pratique, on choisit un nombre premier long de 300 chiffres environ).

Bob et Alice appliquent leurs fonctions à sens unique à une suite de bits publique (*en haut*). Dans un cas, Alice applique d'abord sa fonction ; dans l'autre, c'est Bob qui applique sa fonction en premier. Le résultat ne dépend pas de l'ordre d'application, mais les exponentielles compliquent les données au point d'empêcher tout intrus de déterminer les exposants secrets de Bob ou d'Alice, ou la suite de bits finale (la clé) qui leur servira dans les communications futures.

