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 entrait, 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 chevreaux.

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 chevreaux 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 essayent 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 nombreuses 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.

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

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.

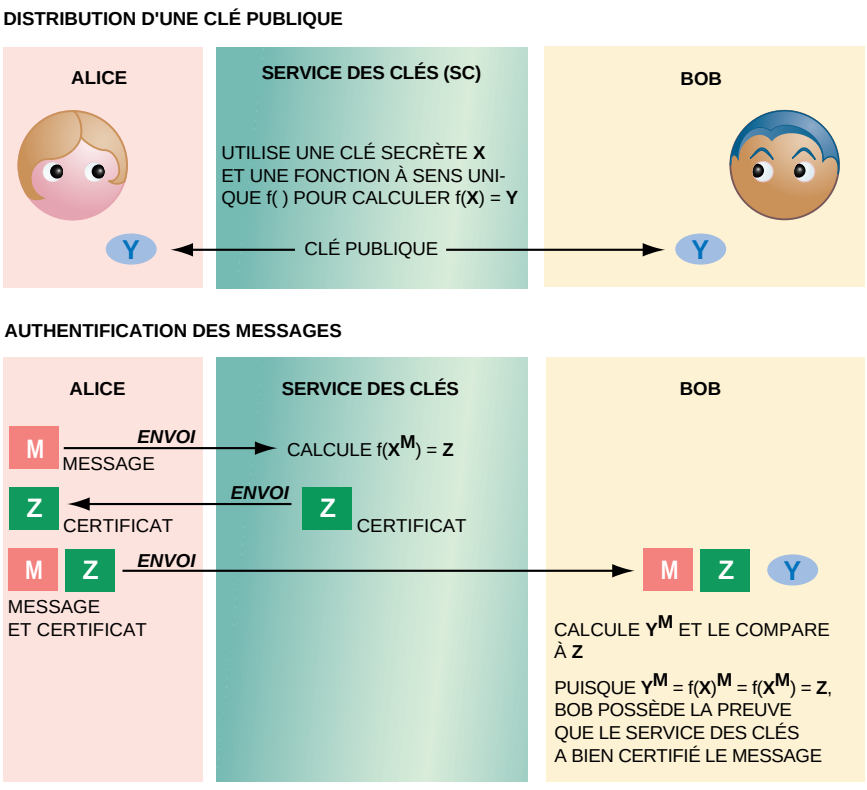
Le système SELANE est utilisable par n'importe quel réseau commercial ou universitaire. Nous avons également créé une carte à puce qui sécurise les opérations nécessaires à chaque utilisateur.

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

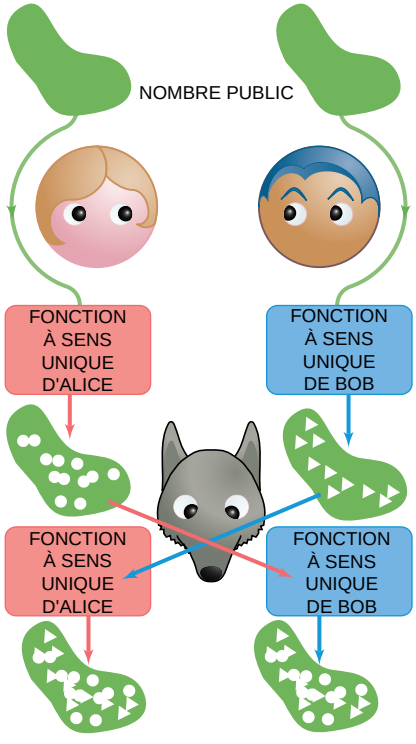


2. LES PROTOCOLES d'authentification reposent sur une séquence secrète de bits connue seulement par l'organisme qui les délivre et sur une succession d'exponentielles. Cet organisme ne publie qu'une version chiffrée de sa séquence secrète, mais il donne la possibilité de vérifier que c'est bien lui qui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

Des fonctions à sens unique pour vaincre les oreilles indiscrètes

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.



souhaitant signer des documents choisit une chaîne de bits secrète et permanente, et publie la transformée de ce nombre par une fonction exponentielle modulaire. La procédure de production de signature d'un document est la suivante :

• choisir un jeton secret utilisable une seule fois (un nombre),

• appliquer une fonction exponentielle modulaire à ce nombre pour en obtenir un témoin,

• former et résoudre une équation qui utilise les valeurs numériques du message à envoyer, la signature secrète, le jeton et son témoin,

• transmettre le document,

• ajouter sa signature composée du témoin et de la solution de l'équation.

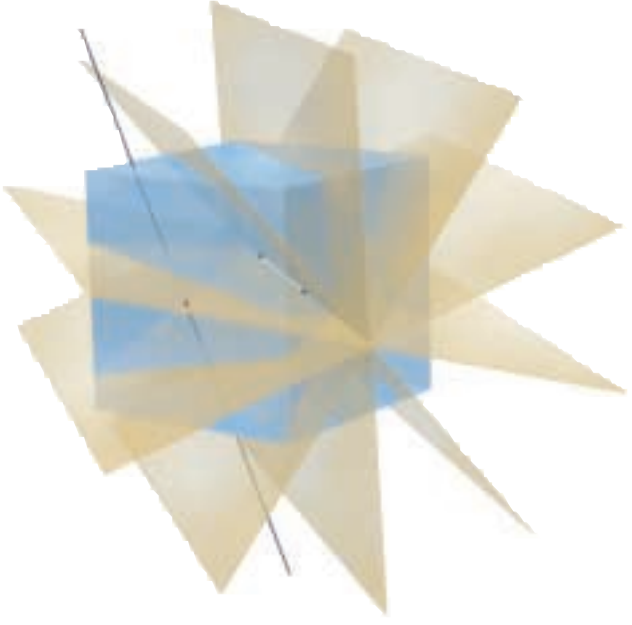
Ainsi n'importe qui peut vérifier que les nombres qui constituent la signature sont bien engendrés par la chaîne privée et par le document émis. Ces dix dernières années, de nombreuses versions de cette technique ont été mises au point.

À la place de cette technique, nous avons cherché comment, pour chaque réseau local d'ordinateur, un service

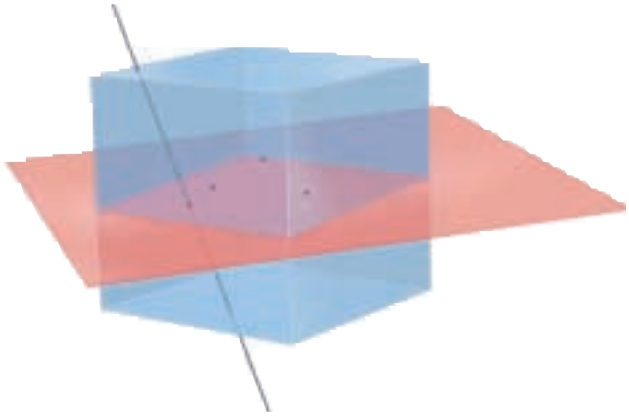
Quand les écoutes téléphoniques deviennent nécessaires

Les techniques de chiffrement que nous avons mises au point satisfont à la fois les particuliers, qui veulent conserver la confidentialité de leurs messages, et les services de police, qui veulent surveiller les échanges. Craignant que les écoutes téléphoniques ne puissent capter que des messages inintelligibles, le gouvernement des États-Unis a réglementé l'utilisation et l'exportation des logiciels de chiffrement. Il promeut également un réseau téléphonique sécurisé qui utilise une puce de chiffrement nommée *Clipper*. Le gouvernement contrôle les clés de cette puce, qui peuvent être obtenues sur demande par des agents officiels. Les détails de ce réseau demeurent secrets. Ce réseau n'inspire guère confiance, car les clés, partagées par les services de police de plusieurs pays, seront difficilement gardées. Ensuite, il peut exister des méthodes de déchiffrement en dehors du cadre des services de police.

En revanche, les méthodes que nous avons mises au point à Karlsruhe peuvent servir de base à un système qui mettrait les utilisateurs et les experts gouvernementaux en cryptographie sur un pied d'égalité. Il fournit un outil puissant pour les échanges de clés et l'authentification qui pourrait fonctionner avec le circuit *Clipper* ou avec d'autres dispositifs de chiffrement plus robustes. Afin d'augmenter la confiance accordée au procédé, on pourrait établir des clés numériques nécessitant la coopération de différents services pour autoriser les écoutes téléphoniques.



LA CONNAISSANCE DE TROIS POINTS peut être répartie entre plusieurs personnes, de manière qu'aucune d'entre elles ne puisse, à elle seule, déduire un point secret. Il existe en effet une infinité de plans passant par deux points confiés à chacune des personnes.



À PARTIR DES DONNÉES DE TROIS POINTS (un plan) et d'une droite publique, on calcule les coordonnées du point d'intersection. Ces coordonnées forment une clé secrète à trois parties.

Pour comprendre comment ce garde-fou pourrait fonctionner, imaginons que la séquence de bits qui code la clé soit constituée non pas d'un seul nombre, mais de trois ou plus. Gustavus Simmons, des Laboratoires *Sandia*, a eu l'idée d'utiliser trois fractions de la clé secrète comme coordonnées d'un point dans un espace à trois dimensions.

Toute clé secrète serait composée de trois nombres appartenant à une droite dans cet espace. Cette droite, connue de tous, serait néanmoins sûre en raison du nombre infini de ses points. On effectuerait le partage de l'information concernant le point secret en faisant passer un plan par ce point et en choisissant trois autres points au hasard sur ce plan. Ces points seraient utilisés pour reconstruire le plan et trouver son intersection avec la droite.

Chacun des membres de la commission d'autorisation des écoutes téléphoniques recevrait les coordonnées de deux des points. Deux membres en accord pourraient alors déterminer le point secret. Toutefois, grâce à SELANE, ils obtiendraient les coordonnées précises sans connaître le nombre secret, ce qui compromettrait la sécurité du système. S'ils donnent à leurs partenaires la version chiffrée de leur point, la même relation mathématique existera entre ces points et l'image de la droite codée qu'entre les vrais points et la véritable droite sur laquelle se trouve le point secret.

Ce principe est généralisable quelle que soit la taille de la commission et le quorum nécessaire. Des responsabilités partagées de cette façon compliquent n'importe quelle tentative de percer le secret, que ce soit par la violence, le chantage ou la corruption. Je pense que le monde des affaires accepterait volontiers un tel système, qui éviterait la mainmise de l'État. Les gouvernements pourraient également l'accepter pour éviter la prolifération des codages robustes, ce qui se produit aujourd'hui.

des clés pourrait remplacer les services de délivrance des passeports. Avant d'attribuer le premier identificateur, le service des clés élabore ses propres clés de signature : un nombre secret et la version publique, obtenue à l'aide d'une exponentielle modulaire. Quiconque désire vérifier les identificateurs attribués par le service des clés a juste besoin d'une copie de la clé publique.

Le service des clés fournit un certificat (une puce électronique résistant aux altérations et placée dans une carte de crédit ou dans une montre spéciale) à chaque personne, terminal ou ordinateur de son réseau. Ce certificat peut être utilisé dans toutes les transactions. Lorsque Alice demande un numéro d'identification au service des clés, elle obtient un certificat dont la mémoire contient le message suivant : «Le propriétaire de cette carte est Alice Wunderkind, professeur d'informatique à l'Université de Paris», suivi d'une signature du type ElGamal fondée sur ce message.

Ultérieurement, afin de convaincre Bob que son numéro d'identification est valide, Alice utilise son certificat pour lui envoyer un message ainsi que le témoin du jeton utilisé dans la signature. En utilisant ces valeurs et la clé publique du service des clés, Bob calcule le partie de la signature que le certificat n'a pas révélé. Pour s'assurer que l'identificateur est valide, Bob dialogue avec le certificat en lui posant des questions dont les réponses sont justes seulement s'il connaît la partie secrète de la signature.

Mes collègues et moi-même avons conçu un protocole qui intègre l'authentification et la vérification avec l'échange des clés. Ce protocole est exécuté en une fraction de seconde par un microprocesseur placé dans une carte à puce. Si leurs numéros d'identification sont bons, les deux partenaires terminent leur premier échange par une clé commune qui servira dans les transactions futures. Si l'authentification échoue, chacun reçoit une séquence différente, sans utilité aucune.

Chaîne de confidentialité

Cette méthode d'identification repose sur la confiance que Bob accorde au service de délivrance des clés d'Alice. Pour vérifier le numéro d'identification, on devra connaître la signature de tous les services des clés. Dans le cas des transactions internationales, cette méthode n'est utilisable que si les services des clés sont hiérarchisés : chacun d'entre eux devrait se légitimer en se procurant un identificateur d'un service des clés supérieur.

Une station de distribution centrale devrait garantir la confiance que l'on accorde à chacun des services des clés universitaires, qui, à leur tour, garantiraient les services des clés internes. Ce schéma est extensible à un nombre quelconque de niveaux. Une station centrale française pourrait se légitimer en utilisant l'identificateur numérique d'un centre européen qui, à son tour, serait validé par une organisation mondiale. La carte à puce détenue par une personne pourrait contenir une cascade de messages : une identification individuelle signée par le service des clés local, une identification de l'institution signée par l'autorité régionale, et ainsi de suite. La vérification d'un identificateur ne nécessite de connaître que la signature numérique d'un petit nombre d'autorités et de leur faire confiance. Ainsi pourrait-on échanger des informations à distance avec autant de confiance que si le correspondant était présent.

Thomas BETH est professeur d'informatique à l'Université de Karlsruhe et directeur de l'Institut européen des systèmes de sécurité.

Taher ELGAMAL, *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, in *IEEE Transactions on Information Theory*, vol. 31, n° 4, pp. 469-472, juillet 1985.

T. BETH, *Efficient Zero-Knowledge Identification Scheme for Smart Cards*, in *Advances in Cryptology : EUROCRYPT '88*, sous la direction de Christoph Günther, Springer-Verlag, 1988.

Public-Key Cryptography : State of the Art and Future Directions, sous la direction de T. Beth, M. Frisch et G.J. Simmons, Springer-Verlag, 1992.

Gustavus J. SIMMONS, *Contemporary Cryptology : The Science of Information Integrity*, IEEE Press, 1992.

T. BETH, *Keeping Secrets a Personal Matter or the Exponential Security System*, in *Cryptography and Coding III*, sous la direction de M.J. Ganley, Oxford University Press, 1993.

H. DANISCH, *RFC 1824 : The Exponential Security System TESS* in European Institute for System Security World Wide Web site at http : / / avalon.ira.uka.de / eiss / indexe.html.