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.

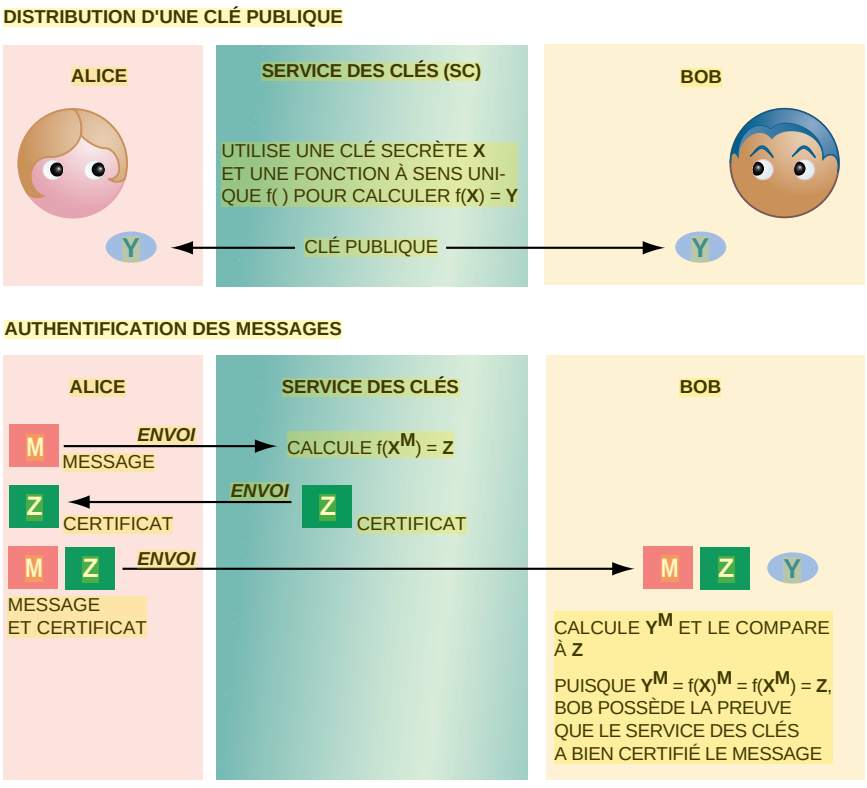
Le système SELANE est utilisable par n'importe quel réseau commercial ou universitaire. Nous avons également créé une carte à puce qui sécurise les opérations nécessaires à chaque utilisateur.

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

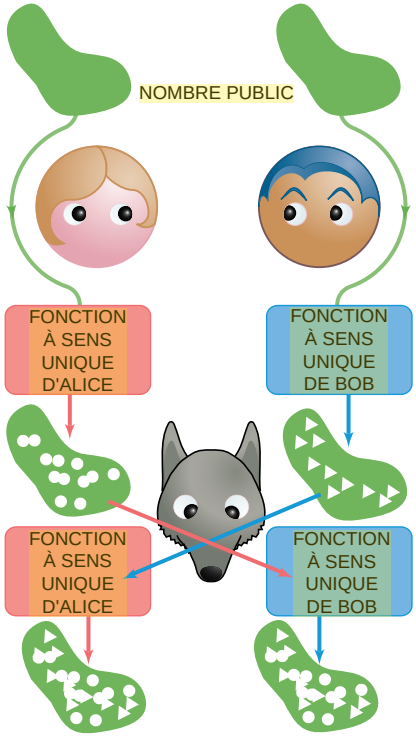


2. LES PROTOCOLES d'authentification reposent sur une séquence secrète de bits connue seulement par l'organisme qui les délivre et sur une succession d'exponentielles. Cet organisme ne publie qu'une version chiffrée de sa séquence secrète, mais il donne la possibilité de vérifier que c'est bien lui qui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

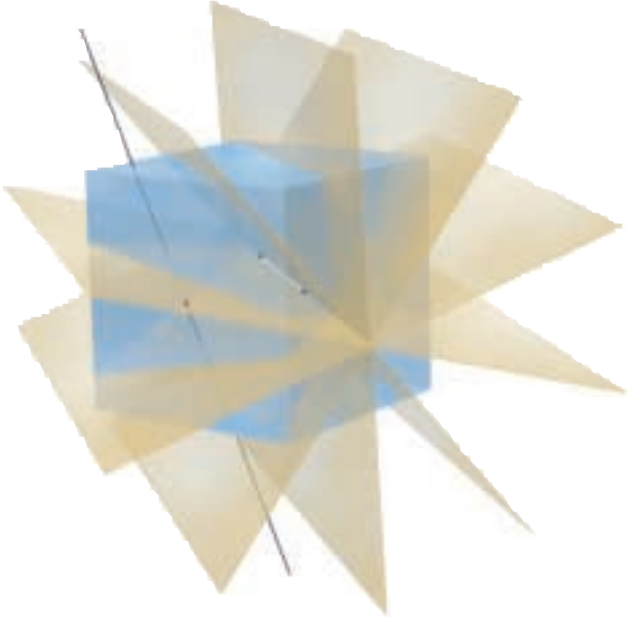
Ainsi n'importe qui peut vérifier que les nombres qui constituent la signature sont bien engendrés par la chaîne privée et par le document émis. Ces dix dernières années, de nombreuses versions de cette technique ont été mises au point.

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

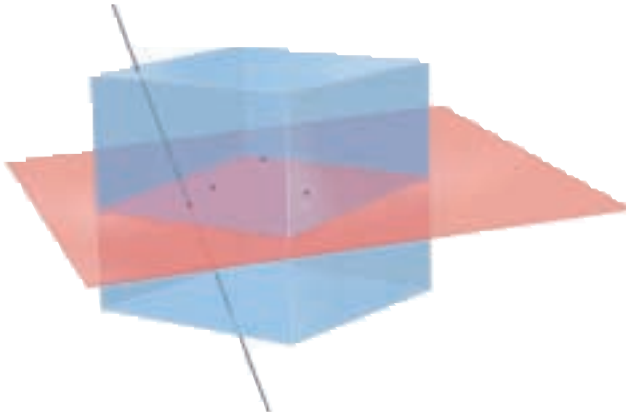
Quand les écoutes téléphoniques deviennent nécessaires

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.