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.

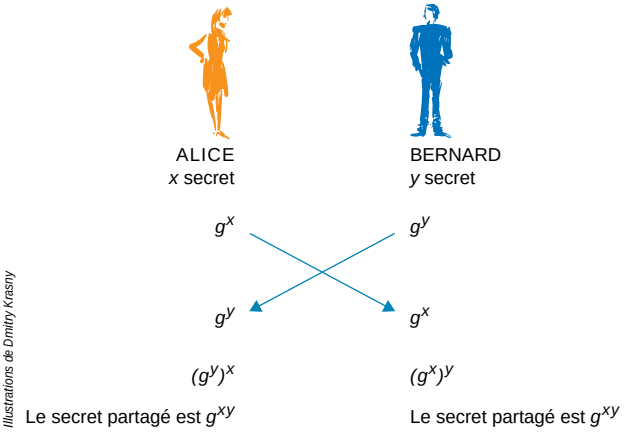
Avec les algorithmes à clé publique, le destinataire peut connaître l'identité de l'expéditeur. Lorsque Bernard envoie

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.

un message à Alice, il le chiffre avec sa clé secrète, puis il chiffre le résultat en utilisant la clé publique d'Alice. À la réception, Alice effectue les étapes inverses : elle déchiffre le message avec sa clé secrète, puis elle déchiffre le résultat avec la clé publique de Bernard. Si elle parvient à lire le message, elle est certaine que c'est bien Bernard qui l'a écrit.

Ces opérations de chiffrement et de déchiffrement nécessitent des myriades d'opérations mathématiques, mais des logiciels exécutables par des ordinateurs personnels automatisent le processus ; l'utilisateur n'a qu'à cliquer sur les boutons «chiffrer» ou «déchiffrer» (ainsi mon programme PGP, l'acronyme de *Pretty Good Privacy*, soit «confidentialité raisonnable», est distribué gratuitement sur le réseau Internet ; son utilisation en France est maintenant autorisée).

Cryptographie à clé publique



Illustrations de Dmitry Krasny

Pendant des siècles, la cryptographie a été handicapée par le problème de l'échange des clés. Supposons que Bernard ait envoyé un message chiffré à Alice. Cette dernière ne pourra lire le message que si elle reçoit également la clé de codage. Les systèmes cryptographiques à clé publique évitent cet envoi, grâce à l'utilisation de mathématiques ingénieuses.

Avec l'algorithme de Diffie et Hellman, Alice utilise son nombre secret x pour calculer g^x (où g est un nombre public) et elle envoie cette valeur à Bernard. De son côté, Bernard utilise son nombre secret y pour calculer g^y et envoie le résultat à Alice. À la réception, Alice peut alors calculer $(g^y)^x$, tandis que Bernard calcule le même nombre $(g^x)^y$. Cette quantité devient leur clé secrète partagée.

Un intrus qui aurait intercepté la valeur g^x d'Alice, ainsi que la valeur g^y de Bernard peut en déduire les valeurs secrètes de x et de y. Aussi, pour déjouer toute indiscrétion, Alice et Bernard utilisent la fonction modulo, qui donne le reste d'une division (par exemple, 14 modulo 4 est égal à 2 : le reste de la division de 14 par 4 est égal à 2). Cette astuce assure le secret, car, au lieu d'envoyer g^x à Bernard, Alice lui transmet le nombre g^x modulo p, à partir duquel un pirate aura bien du mal à retrouver x, même s'il connaît g et p.

En compliquant l'algorithme de Diffie et Hellman, on a obtenu des systèmes qui engendrent deux clés complémentaires, l'une secrète (x pour Alice) et l'autre publique (à savoir g, p et g^x modulo p). La clé secrète déchiffre le message chiffré par la clé publique, mais la clé utilisée pour chiffrer un message ne peut être utilisée pour le déchiffrer. Ainsi, Bernard peut utiliser la clé publique d'Alice (qu'elle a donnée à tout le monde) pour chiffrer un message qui lui est destiné, mais seule Alice peut déchiffrer ce message à l'aide de sa clé secrète.

Malgré ces progrès, la cryptographie à clé publique a deux graves limitations. D'une part, la technique est relativement lente, de sorte qu'en pratique on ne peut chiffrer les messages trop longs. D'autre part, des structures caractéristiques du message en clair subsistent dans le message chiffré. Détectables dans le texte chiffré, ces fragments sont utilisables par des spécialistes, qui peuvent reconstituer la totalité des messages.

Chevaux de bataille symétriques

Pour ces raisons, le chiffrement est souvent assuré par des techniques symétriques, plus rapides et plus sûres, et la cryptographie à clé publique ne sert que lors de l'étape d'échange des clés symétriques. Par exemple, Bernard chiffre son message avec une clé symétrique rapide et sûre. Comme il doit envoyer à Alice la clé qu'il a utilisée, il la chiffre avec la clé publique d'Alice et attache le résultat à son message chiffré. Alice pourra déchiffrer la clé symétrique en utilisant sa clé secrète. Muni de la clé symétrique, elle déchiffrera alors le reste du message de Bernard.

Pour authentifier ses messages, Bernard ne les signe pas non plus à l'aide des techniques à clé publique ; il extrait du message un condensé numérique, ou «empreinte digitale», à l'aide d'une transformation mathématique, nommée fonction de hachage. Cette transformation associe à un message de longueur quelconque un message de longueur fixe, telle que 160 bits (un bit est un chiffre binaire, égal à 0 ou à 1). Les programmes cryptographiques sont conçus de manière que deux messages différents n'aient pas le même condensé. Autrement dit, l'empreinte digitale est unique, deux messages différents ayant à peu près certainement deux condensés différents.

Après avoir calculé le condensé de son message, Bernard le chiffre avec sa clé secrète. Il envoie cette «signature» en même temps que le reste de son message chiffré. Lorsqu'elle reçoit ce condensé chiffré, Alice le déchiffre grâce à la clé publique de Bernard. Elle compare alors le résultat obtenu avec le résultat qu'elle calcule elle-même après déchiffrement du message. Si les deux résultats sont identiques, elle conclut que le message n'a pas été modifié et que Bernard en est bien l'expéditeur.

Pour chiffrer un message destiné à circuler sur le réseau Internet, on le découpe souvent en blocs de taille fixe (généralement 64 ou 128 bits), puis on chiffre individuellement les blocs successifs. Ce système de chiffrement par blocs crypte plusieurs fois chaque bloc (le nombre d'itérations dépend des algorithmes utilisés). Chaque itération fait intervenir des permutations circulaires (la permutation d'un groupe de trois blocs «xtv» devient «tvx») et des substitutions («tvx» engendre «cb2»). Une partie de la clé participe à la transformation des données au cours de chaque itération.

Quand on fournit des morceaux de texte identiques à un système de chiffrement, on obtient des blocs identiques. Aussi, afin d'éviter le maintien de structures qui faciliteraient la découverte du message, les algorithmes par blocs utilisent un chaînage : les blocs qui viennent d'être chiffrés servent à déchiffrer les blocs suivants. Le chiffrement d'un bloc de texte dépend alors de tous les blocs qui le précèdent.

La longueur des clés de chiffrement par blocs est généralement égale à 56, 128 ou 256 bits. Les méthodes les plus connues sont DES (*Data Encryption Standard*, soit

«standard de chiffrement de données»), triple-DES, CAST, IDEA et *Skipjack*. Les algorithmes par blocs sont au centre de la plupart des recherches actuelles en cryptographie.

La clé est la clé

En cryptographie, l'étape la plus sensible est la création des clés. Pour qu'un système soit le plus sûr possible, les clés doivent être des nombres réellement aléatoires, imprévisibles par un éventuel pirate. Les séquences pseudo-aléatoires déterministes que les ordinateurs engendrent pour les jeux ou les simulations sont inutilisables, car ils sont insuffisamment aléatoires. La seule manière d'engendrer de vrais nombres aléatoires est d'utiliser un «bruit» physique, telle la désintégration radioactive.

À l'aide d'un ordinateur, on fabrique difficilement des nombres aléatoires aussi bons que ceux issus de la physique. On obtient toutefois des résultats raisonnables quand on utilise l'intervalle de temps, en microsecondes, qui sépare la frappe de deux touches d'un clavier : cette valeur est impossible à prédire. Les données obtenues ainsi ne sont pas assez aléatoires pour fabriquer directement des clés, mais peuvent être transformées pour accroître le désordre.

La seule méthode cryptographique dont on ait prouvé la parfaite sécurité est le chiffrement de Vernam, où la longueur de la clé est égale à la longueur du message. Dans cette méthode, on utilise une séquence aléatoire pour chiffrer le message bit par bit, c'est-à-dire que le 34e bit de la clé code le 34e bit du message. La clé doit être parfaitement aléatoire, elle ne peut pas être une séquence pseudo-aléatoire issue d'un algorithme déterministe, sinon le code pourrait facilement être cassé. Le chiffrement de Vernam est rarement utilisé, en raison de difficultés pratiques : la clé, qui est aussi longue que le message, doit être envoyée au destinataire par un canal de transmission sûr. De surcroît, on ne peut utiliser chaque clé qu'une seule fois, sinon un pirate pourrait la décrypter.

Si la taille des clés détermine l'efficacité des systèmes cryptographiques, la conception des systèmes est également très importante. Considérons un simple code de substitution où tous les A seraient transformés en W, tous les B en K, tous les C en Q, et ainsi de suite. Le nombre de façons différentes d'arranger l'alphabet est égale à 26! (ce nombre, qui se lit «factorielle 26», est égal à $26 \times 25 \times 24 \ldots 3 \times 2 \times 1$), soit environ 4×10^{26} (un nombre de 26 chiffres)! On ne peut tester toutes les combinaisons une à une, mais, lorsque j'étais enfant, je m'amusais à casser ce type de code avec un papier et un crayon : je regardais simplement la lettre la plus fréquente et je supposais qu'il s'agissait d'un E ; puis je cherchais la deuxième lettre la plus fréquente et je supposais que c'était un S, etc. Ainsi, malgré un espace des clés très grand, ce type de code est très simple.

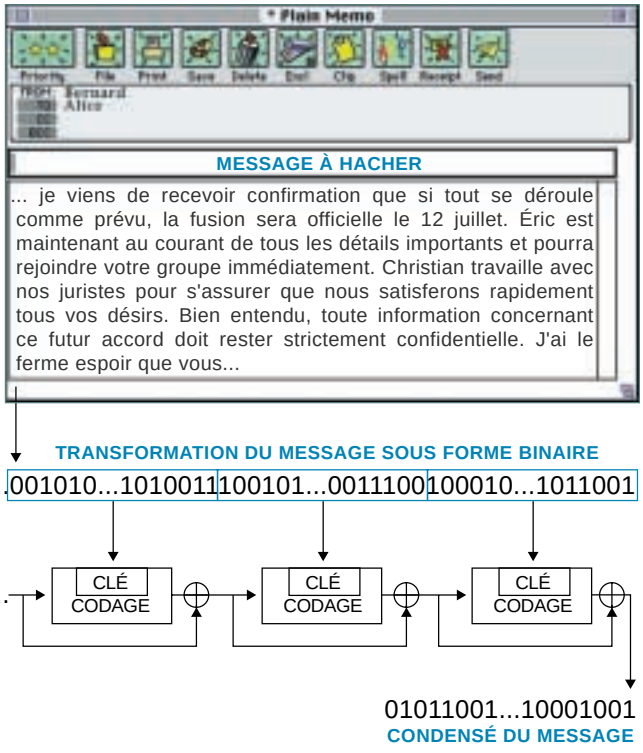
En fait, la sécurité d'un système cryptographique n'est pas proportionnelle à la taille de la clé. Pour les systèmes par blocs, par exemple, la relation est plutôt exponentielle : un bit de plus à la clé oblige un pirate éventuel à doubler le nombre d'essais. L'effort nécessaire est élevé au carré quand la taille de la clé est doublée. Pour casser un système qui utilise une clé de longueur 128 bits, il faut en moyenne 2^{127} (soit $1{,}7 \times 10^{38}$) opérations.

Pour les algorithmes à clé publique, la difficulté augmente plus lentement. L'espace des clés augmente moins vite qu'une loi exponentielle, mais plus vite qu'une loi de puissance ; le doublement de la longueur de la clé n'élève pas au carré l'effort à fournir pour casser le code, mais le travail reste considérable. Par exemple, dans le système RSA, les algorithmes modernes de factorisation peuvent faire beaucoup mieux que d'essayer toutes les combinaisons de nombres premiers possibles pour factoriser un nombre de grande taille. Le code de Diffie et Hellman est, lui aussi, «sous-exponentiel». Par exemple, une clé de 3 000 bits pour RSA ou Diffie-Hellman est aussi difficile à décrypter qu'une clé de 128 bits d'un système de chiffrement par blocs.

Le chiffrement par blocs n'est toutefois pas invulnérable. En 1998, la Société *Electronic Frontier Foundation* a construit, pour moins de 1,5 million de francs, un ordinateur massivement parallèle qui a cassé un message chiffré par DES en explorant toutes les clés à 56 bits en moins d'une semaine.

La force brute n'est pas la seule façon de percer un code. Des méthodes mathématiques élaborées et des outils statistiques raccourcissent le travail. Certaines méthodes recherchent, par exemple, un motif particulier dans le message chiffré. Ces méthodes statistiques sont classées en trois catégories selon ce qui est connu du texte clair et du texte chiffré.

Quand le pirate connaît seulement le texte chiffré, il n'a rien pour le guider dans sa recherche de la clé, si bien que même un système simple de chiffrement résiste aux



2. UNE FONCTION DE HACHAGE crée un condensé de message, semblable à une empreinte digitale utilisée pour détecter les contrefaçons. Le texte d'un message est d'abord converti en chiffres binaires (la lettre A peut être représentée par 00000, la lettre B par 00001, le C par 00010, etc.) ; puis la suite de caractères qui en résulte est découpée en blocs de taille fixe. Chacun des blocs sert alors de clé dans un système de codage. La sortie finale est le condensé du message original. Quelle que soit la longueur du message initial, le condensé a toujours la même taille. C'est une opération à sens unique, car il est quasi impossible de retrouver le message original à partir de son condensé. De surcroît, avec cet algorithme, deux messages donnent presque toujours des condensés différents et il est impossible de trouver un autre message ayant le même condensé : ce condensé est une «empreinte digitale» du message.

assauts. En revanche, quand le pirate connaît au moins une partie du message, ses chances de succès augmentent. Par exemple, s'il sait qu'il commence par «Cher Monsieur Dupond», il peut d'abord chercher une clé qui décrypte la partie «Cher Monsieur Dupond» du texte clair, puis poursuivre le décryptage à l'aide des informations trouvées. Même quand le pirate ne connaît que le langage utilisé dans le texte clair, russe, français ou COBOL, il peut exploiter cette information. Si le message est en français, par exemple, alors le mot le plus fréquemment utilisé est sans doute «le» ou «la». Pour déjouer de telles attaques, certains systèmes cryptographiques compriment le message en clair,

L e s

Les certificats numériques sont importants en cryptographie à clé publique, parce qu'ils garantissent qu'un intermédiaire n'espionne pas les échanges. Pour envoyer ou recevoir des messages en utilisant les clés publiques, un utilisateur doit posséder deux clés cryptographiques, l'une secrète, l'autre publique. Ces clés sont de longues suites de 0 et de 1 (entre 500 et 1 000 chiffres binaires). L'utilisateur garde sa clé secrète dans un endroit sûr, chiffrée sur un disque dur par exemple, mais il distribue sa clé publique à ceux avec qui il veut communiquer.

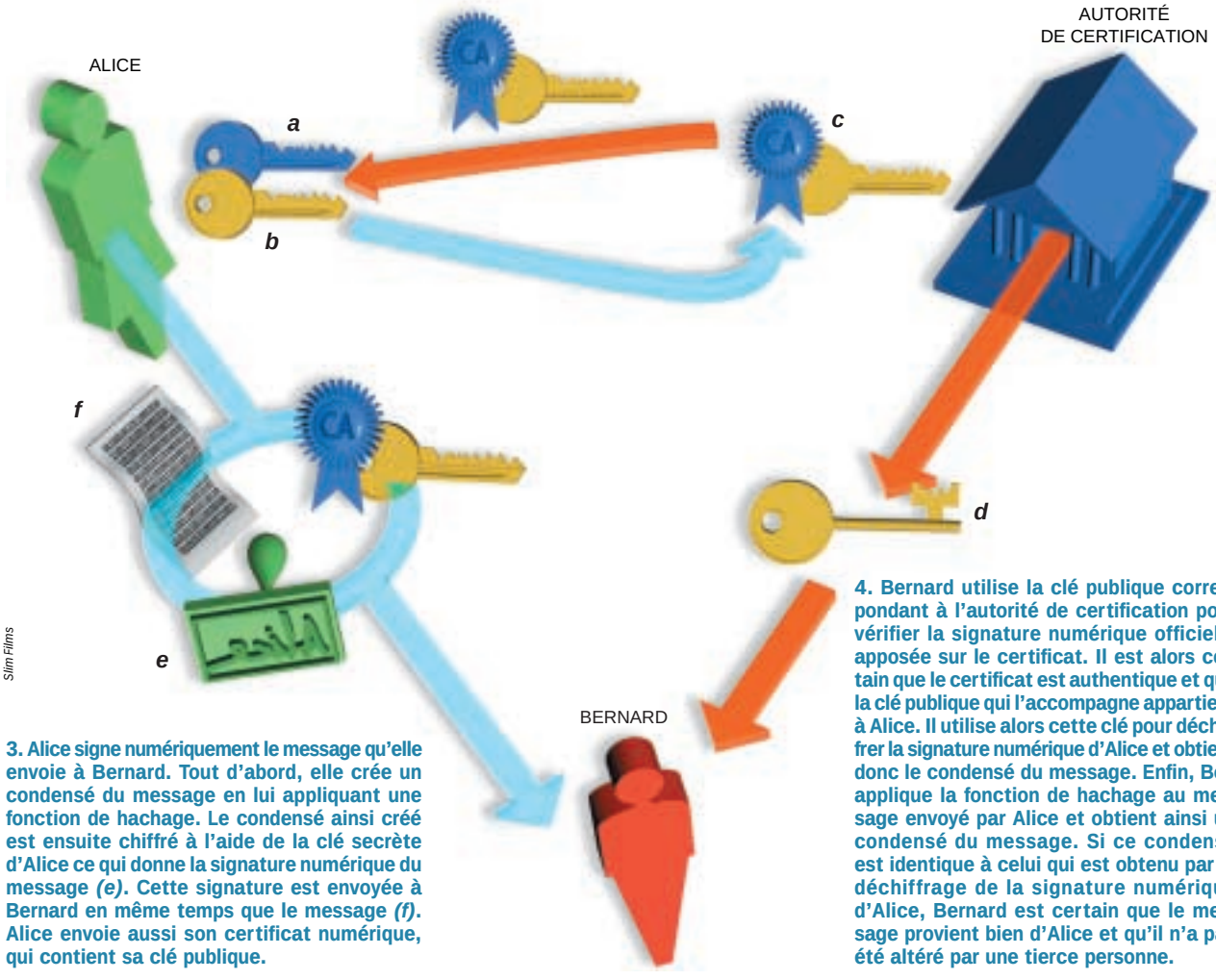
Supposons qu'Alice veuille envoyer à Bernard un message authentifié, c'est-à-dire un message dont Bernard saura de façon certaine qu'il vient d'elle. En utilisant sa clé secrète, Alice crée une signature numérique qu'elle joindra au message. Puis, en utilisant la clé publique d'Alice, Bernard vérifiera cette signature. Cependant, comment Bernard saura-t-il que la clé publique appartient effectivement à Alice ?

Un imposteur pourrait créer sa propre paire de clés et envoyer sa clé publique à Bernard en prétendant qu'elle appartient à Alice. On évite cette fraude en utilisant une autorité de certification, qui fournira un certificat numérique sur la clé publique reconnu par tous. Plusieurs entreprises, telles *VeriSign* ou *GTE CyberTrust*, délivrent des certificats numériques. Ainsi, le certificat numérique est l'analogue informatique de la carte d'identité.

Warwick FORD, *VeriSign*

1. À l'aide des logiciels de cryptographie, Alice crée une clé secrète *(a)* ainsi qu'une clé publique *(b)*. Elle envoie la clé publique à une autorité de certification, à qui elle demande un certificat numérique. Pour authentifier Alice, cet organisme vérifie les informations fournies par Alice. Si tout est en ordre, l'organisme de certification envoie un certificat numérique *(c)* qui authentifie la clé publique d'Alice. Sur ce certificat se trouve la signature numérique du tiers de confiance qui peut être vérifiée par toute personne connaissant la clé publique de cet organisme.

2. La clé publique *(d)* de l'autorité de certification est fournie à ceux qui en ont besoin, dont Bernard. Elle peut être incluse dans les programmes de navigation sur le réseau Internet et dans d'autres logiciels utilisés pour les communications informatiques sécurisées.



3. Alice signe numériquement le message qu'elle envoie à Bernard. Tout d'abord, elle crée un condensé du message en lui appliquant une fonction de hachage. Le condensé ainsi créé est ensuite chiffré à l'aide de la clé secrète d'Alice ce qui donne la signature numérique du message *(e)*. Cette signature est envoyée à Bernard en même temps que le message *(f)*. Alice envoie aussi son certificat numérique, qui contient sa clé publique.

4. Bernard utilise la clé publique correspondant à l'autorité de certification pour vérifier la signature numérique officielle apposée sur le certificat. Il est alors certain que le certificat est authentique et que la clé publique qui l'accompagne appartient à Alice. Il utilise alors cette clé pour déchiffrer la signature numérique d'Alice et obtient donc le condensé du message. Enfin, Bob applique la fonction de hachage au message envoyé par Alice et obtient ainsi un condensé du message. Si ce condensé est identique à celui qui est obtenu par le déchiffrage de la signature numérique d'Alice, Bernard est certain que le message provient bien d'Alice et qu'il n'a pas été altéré par une tierce personne.

préalablement au chiffrement, ce qui en enlève les motifs prédictibles.

Souvent le pirate en connaît bien plus. S'il a volé une carte à puce qui contient un système cryptographique, il peut envoyer à la carte des milliards de messages judicieusement choisis et étudier les messages chiffrés correspondants ; de telles attaques percent facilement les systèmes de chiffrement peu efficaces. Dans le cas des systèmes à clé publique, l'attaquant peut écrire un message, le coder avec la clé publique (connue) et analyser le texte chiffré qui en résulte. Des méthodes d'analyse des systèmes de chiffrement performantes apparaissent depuis peu : ce sont les méthodes différentielles et linéaires. On les a utilisées pour analyser un grand nombre de systèmes de chiffrement par blocs et pour montrer qu'il est possible de décrypter les messages chiffrés à l'aide de l'algorithme DES des centaines ou des milliers de fois plus rapidement que par une recherche exhaustive.

Dans la cryptanalyse différentielle, introduite par A. Shamir et Eli Biham, de l'Institut Weissman, en Israël, on code des paires de messages clairs, où les différences sont convenablement choisies, afin de trouver des différences dans les paires chiffrées. La découverte de ces différences renseigne alors sur la clé. Dans la cryptanalyse linéaire, mise au point par Mitsuru Matsui, de la Société *Mitsubishi*, on recherche les corrélations, même faibles, qui existent entre les textes clairs, les textes chiffrés et les clés. La méthode accumule les statistiques obtenues sur un grand nombre de couples texte clair–texte chiffré, à la recherche de tendances qui donneraient des indices sur la clé.

Attention aux intermédiaires

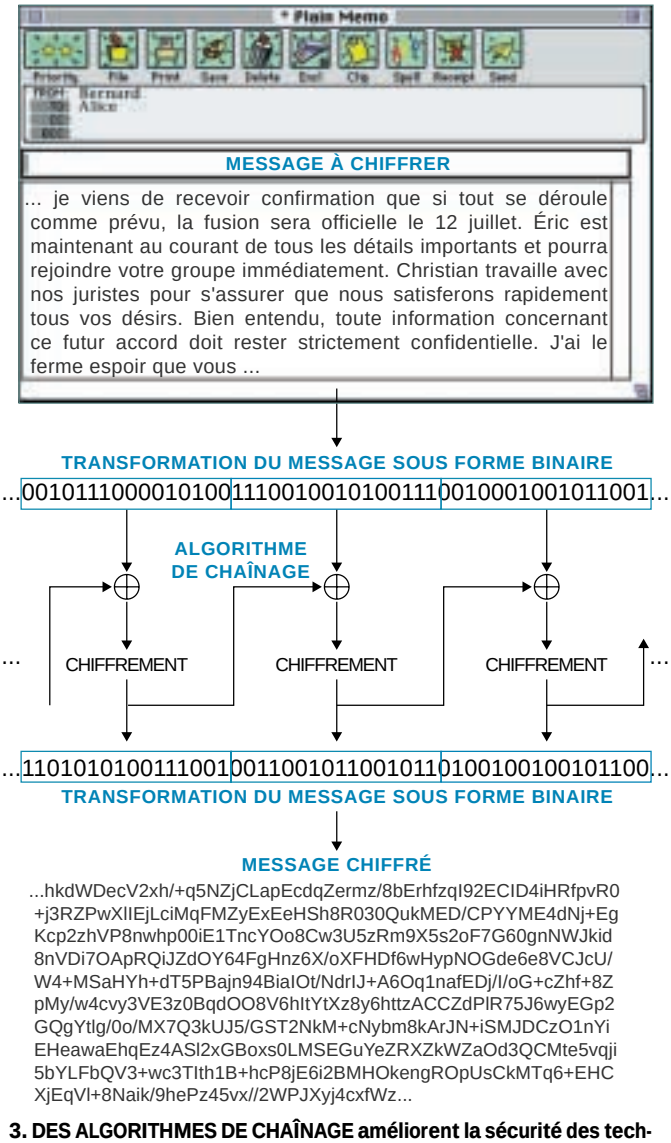
Bien qu'efficaces, les méthodes de cryptanalyse (l'étude de la façon de percer les messages secrets) nécessitent de nombreux calculs. Souvent, au lieu de tenter de casser le système de chiffrement, les pirates préfèrent attaquer son implémentation, car elle laisse parfois «fuir» de l'information. Les systèmes cryptographiques à clé publique sont très vulnérables à une attaque par un tiers qui s'interposerait dans la communication. Bernard, qui envoie un message à Alice, peut ignorer que Caroline s'interpose. Si Caroline parvient à faire croire à Bernard que sa propre clé publique est celle d'Alice, elle pourra déchiffrer les messages émis par Bernard.

Bernard ne peut éviter cette intrusion qu'en s'assurant que la clé utilisée est bien celle d'Alice. La complexité des bons systèmes de cryptographie à clé publique vise presque uniquement à donner cette garantie. Certains systèmes cryptographiques font appel à un tiers de confiance, qui certifie les clés. Toutefois, les clés doivent-elles être certifiées de manière descendante, par des autorités gouvernementales, ou de manière décentralisée, au choix des utilisateurs de systèmes cryptographiques? Ce point fait encore l'objet d'âpres débats.

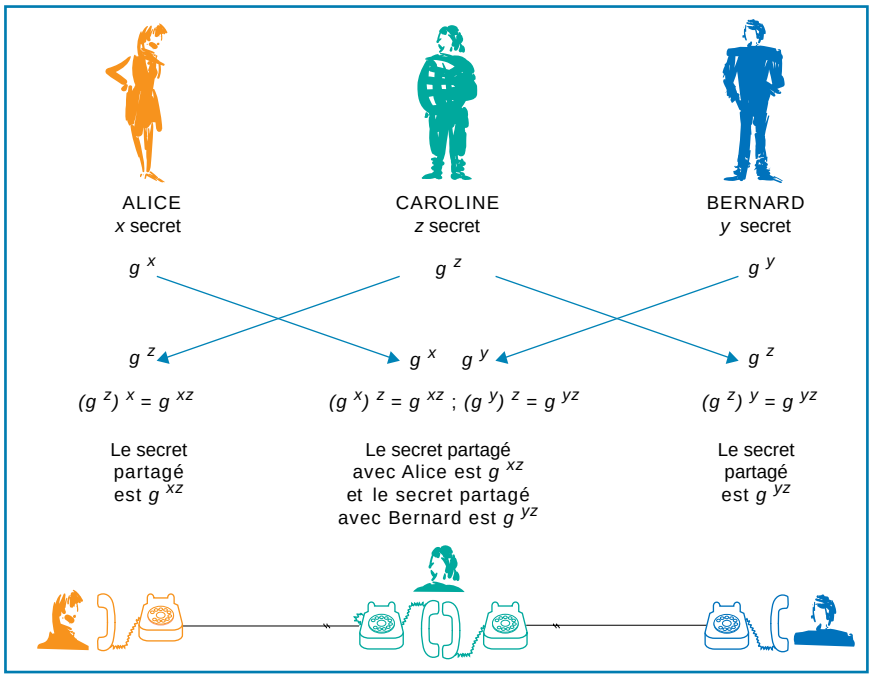
Les algorithmes de cryptographie se sont améliorés en même temps que la cryptanalyse. Le système DES, arrivé en fin de vie, surtout en raison de sa petite clé de 56 bits et de ses blocs de 64 bits, sera remplacé par un nouveau système cryptographique, l'AES (*Advanced Encryption Standard*, soit «standard de chiffrement avancé»). Ce système, qui a mis la communauté de la cryptographie en effervescence, devrait utiliser des clés de 128, 192 ou 256 bits pour chiffrer des données en blocs de 128 bits.

Les systèmes AES devront satisfaire plusieurs contraintes. Ils devront utiliser plusieurs longueurs de clés et de blocs ; ils devront être rapides, créant les clés, chiffrant et déchiffrant les messages à l'aide de processeurs 32 bits, tels ceux qui équipent les ordinateurs personnels, ou de microprocesseurs 8 bits, tels ceux des cartes à puce ; enfin, ils devront fonctionner correctement lors des échanges sur le réseau Internet comme lors des télécommunications par satellite.

Plusieurs propositions d'AES sont intéressantes. Elles bénéficient des études du codage par blocs et des recherches de défense contre les méthodes de cryptanalyses différentielles et linéaires. Plusieurs des 15 systèmes proposés seraient efficaces. Le système MARS, qui dérive du système DES de la Société *IBM*, utilise deux structures très différentes pour chaque itération de chiffrement. Cette approche mixte permet, selon la Société *IBM*, une sécurité



3. DES ALGORITHMES DE CHAÎNAGE améliorent la sécurité des techniques de chiffrements par blocs. On transforme d'abord un message en une chaîne de 0 et de 1 ; puis on découpe cette longue séquence en blocs de même taille. Avant de chiffrer chacun de ces blocs, on le combine mathématiquement avec le bloc chiffré précédent. Ainsi, le chiffrement du 23e bloc dépend du 22e bloc chiffré, qui dépend lui-même du chiffrement du 21e, et ainsi de suite. Le chiffrement d'un bloc dépend alors de tous les blocs précédents.



4. LES SYSTÈMES CRYPTOGRAPHIQUES À CLÉ PUBLIQUE sont vulnérables. Interceptant les transmissions entre Alice et Bernard, l'espionne Caroline dupe Bernard en utilisant son propre g^z à la place du g^x d'Alice et trompe Alice en utilisant g^z à la place du g^y de Bernard *(voir l'encadré de la page 40)*. Elle déchiffre et rechiffre à leur insu les messages qu'ils échangent.

que n'autorisent pas les systèmes de chiffrement classiques. Le procédé CAST-256 est une extension des premières architectures CAST à une clé de 256 bits et à des blocs de 128 bits. Le système *Twofish* est mathématiquement plus rigoureux que *Blowfish*, son prédécesseur. La conception de *Serpent* est fondée sur une structure parallèle inhabituelle, qui le rend aussi rapide que DES et qui permet d'engendrer très rapidement des clés autorisant ainsi son utilisation en tant que fonction de hachage. Au département de mathématiques et d'informatique de l'École normale supérieure, l'équipe de Serge Vaudenay a mis au point le système DFC (*Decorrelated Fast Cipher*, soit «codage décorrélé rapide»), très rapide, et dont on peut prouver la sûreté face à certains types d'attaques.

Déchiffrer le futur

Quelle que soit la proposition sélectionnée, AES avantagera les utilisateurs. Aujourd'hui, les meilleurs systèmes de cryptographie sont supérieurs aux meilleures méthodes de cryptanalyse connues. Bien sûr, la cryptanalyse viendra à bout des nouveaux systèmes, mais de nombreux informaticiens estiment que l'écart entre les méthodes de chiffrement et les méthodes de «cassage» se creusera progressivement.

Je partage cette opinion : la cryptographie civile a grandi dans les universités et dans les entreprises privées, et elle a rattrapé la cryptographie militaire. D'ailleurs, les militaires américains ont rendu public leur système de chiffrement *Skipjack*, qu'ils avaient mis au point en secret. Selon une étude d'Eli Biham, cet algorithme serait moins sûr que les meilleurs algorithmes universitaires. Comme le réseau Internet, la cryptographie est sortie du giron militaire. Souhaitons-lui une croissance aussi remarquable!

Philip ZIMMERMANN est l'auteur du programme de chiffrement PGP (*Pretty Good Privacy*). Il travaille pour la Société *Network Associates*.

Bruce SCHNEIER, *Cryptographie appliquée*, Vuibert, 1996.

Doug STINTON, *Cryptographie : théorie et pratique*, Vuibert, 1996.

G. DUBERTRET, *Initiation à la cryptographie*, Vuibert, 1998.