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.

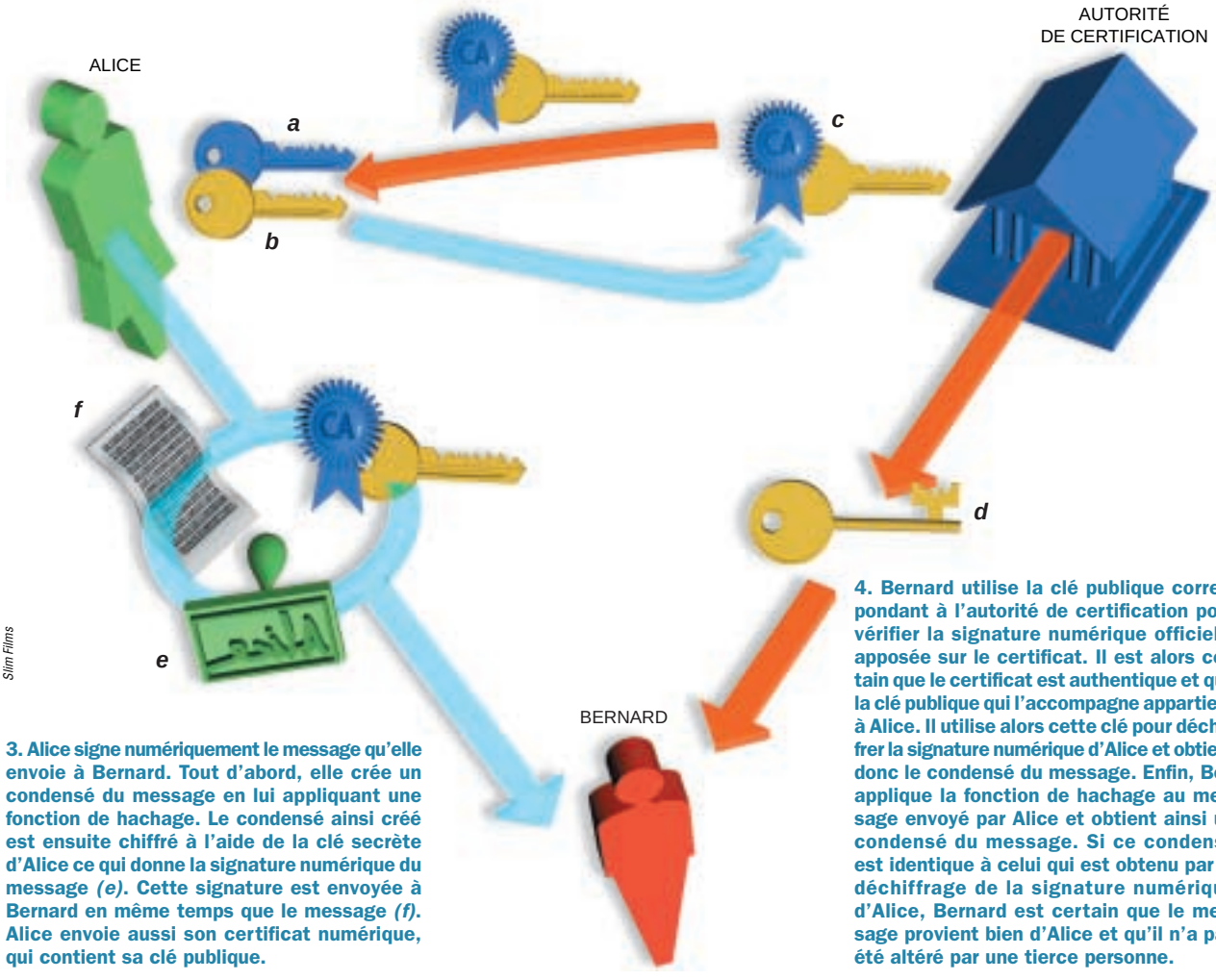
Supposons qu'Alice veuille envoyer à Bernard un message authentifié, c'est-à-dire un message dont Bernard saura de façon certaine qu'il vient d'elle. En utilisant sa clé secrète, Alice crée une signature numérique qu'elle joindra au message. Puis, en utilisant la clé publique d'Alice, Bernard vérifiera 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

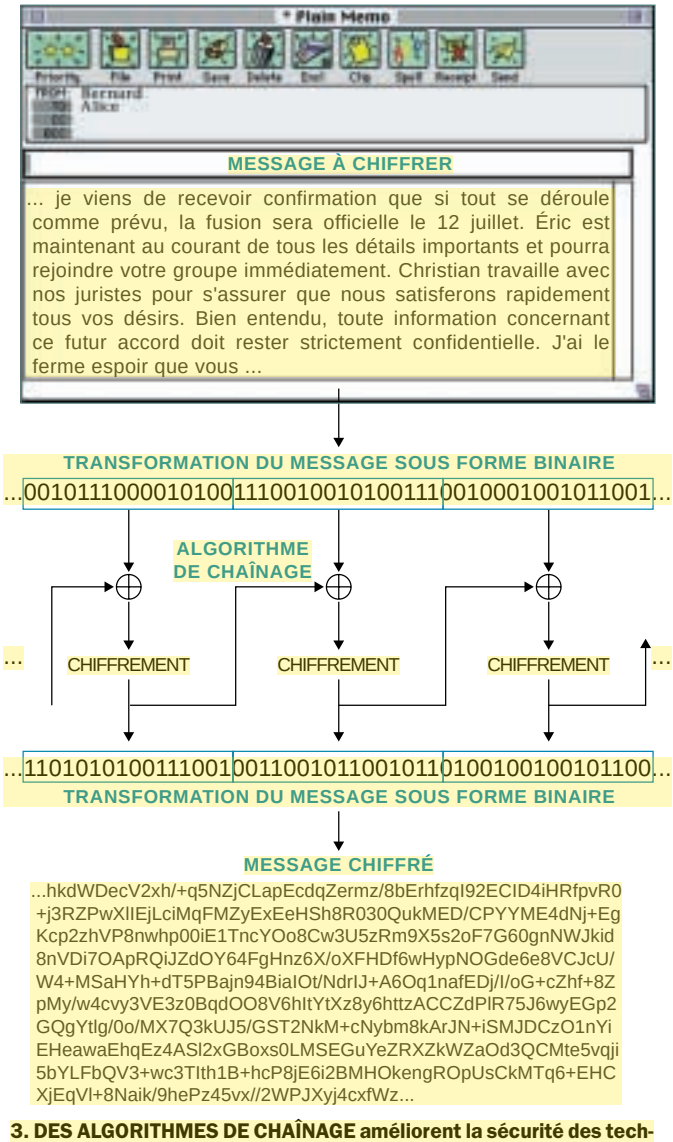
Bien qu'efficaces, les méthodes de cryptanalyse (l'étude de la façon de percer les messages secrets) nécessitent de nombreux calculs. Souvent, au lieu de tenter de casser le système de chiffrement, les pirates préfèrent attaquer son implémentation, car elle laisse parfois «fuir» de l'information. Les 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.

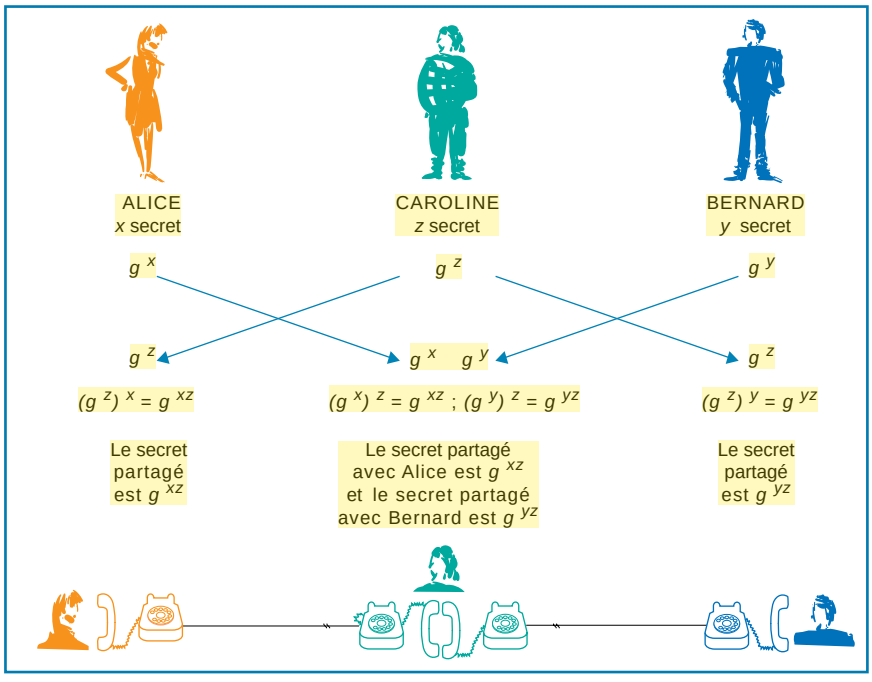
Les algorithmes de cryptographie se sont améliorés en même temps que la cryptanalyse. Le système DES, arrivé en fin de vie, surtout en raison de sa petite clé de 56 bits et de ses blocs de 64 bits, sera remplacé par un nouveau système cryptographique, l'AES (*Advanced Encryption Standard*, soit «standard 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.