Cryptographie

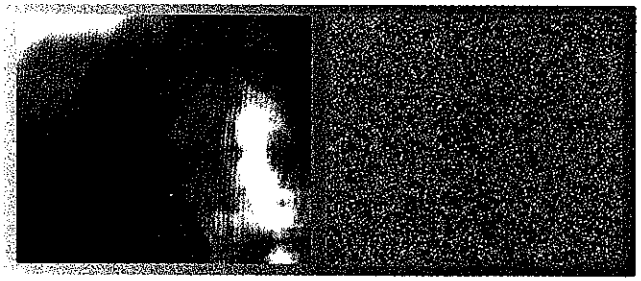
Dans le secret des chiffres

Longtemps réservée aux chefs de guerre et aux agents diplomatiques, la pratique des codes secrets et autres "chiffres" s'est imposée chez tous les usagers des réseaux de télécommunications, Internet notamment. L'échange, via le Web, de données confidentielles, comme les images médicales, exige en effet de trouver des méthodes de cryptage à la fois sûres et rapides. C'est ce à quoi travaillent des mathématiciens et des informaticiens lyonnais et grenoblois.

Hormis celui de Polichinelle, un secret ne vaut en général que s'il est bien gardé. Pour éviter qu'il ne tombe dans des oreilles ou sous des yeux indiscrets, chacun y va de sa méthode. De la confidence chuchotée à l'oreille aux codes les plus élaborés, en passant par les anagrammes ou l'écriture à l'encre invisible, les stratagèmes pour dissimuler un message ou son contenu sont aussi nombreux et variés que leurs utilisateurs.

Il y a d'abord ceux qui le font par devoir, comme les militaires ou les diplomates. Mais il y a aussi et surtout ceux, de plus en plus nombreux, qui communiquent par ordinateurs ou satellites interposés. Pour les détenteurs de cartes bancaires, de téléphones mobiles, ou pour les utilisateurs d'Internet, les codes secrets et autres mots de passe sont devenus indispensables, tant pour accéder aux réseaux de communication que pour protéger leur vie privée. Si bien que la *cryptographie* (ou *cryptologie*), science de l'écriture secrète, fait aujourd'hui appel à des professionnels chevronnés, au premier rang desquels figurent les informaticiens et les mathématiciens.

En effet, les procédés de cryptage ont beaucoup gagné en sûreté et en rapidité grâce à l'arrivée des ordinateurs et aux apports de la recherche en mathématiques (arithmétique, notamment). Mais comme leurs champs d'application ne cessent de s'étendre et qu'ils sont constamment soumis aux assauts des briseurs de codes, il faut en permanence les améliorer ou en inventer de nouveaux.



© CNRS/L. MEDARD

Sans clé de décodage, voici comment apparaîtrait cette image médicale, une fois cryptée.

C'est ce qu'ont entrepris les trois équipes participant au programme "Mathématiques pour la cryptographie et l'imagerie", financé par la Région Rhône-Alpes. *« Nous travaillons avec le laboratoire CREATIS de l'INSA de Lyon, et l'Institut Joseph-Fourier de Grenoble, à la mise au point d'un protocole sécurisé de transmission, via Internet, de dossiers médicaux, plus précisément des images médicales »*, expose Jean-Louis Nicolas, chercheur à l'Institut Girard Desargues de l'Université Lyon 1[1] et coordinateur du projet.

Un subtil jeu de verrous et de clés

Or ce protocole doit répondre à deux exigences : préserver la confidentialité des données, et garantir au destinataire que ces données n'ont subi aucune modification – accidentelle ou malveillante – au cours du transfert (c'est crucial en imagerie médicale !). En outre, les dossiers étant assez volumineux – une image médicale, une fois numérisée, représente en moyenne 10 mégaoctets de données, soit le volume d'environ 7 disquettes –, il faut éviter que les opérations de chiffrement (codage) et de déchiffrement (décodage) ralentissent la transmission.

Hélas, les procédés de cryptographie les plus sûrs sont aussi… les plus lents. Ainsi, le système actuellement le plus robuste, appelé RSA (du nom de ses inventeurs *Rivest, Shamir* et *Adleman*), est 100 à 1 000 fois plus lent que la norme de codage AES (*Advanced Encryption System*) !

La raison en est simple. *« Tout système cryptographique repose sur des verrous et des clés,* explique Jean-Louis Nicolas. *Le verrou, c'est "l'algorithme de chiffrement", c'est-à-dire la suite d'opérations à effectuer pour obtenir le message codé – par exemple, remplacer les lettres d'un mot par des nombres. La clé, c'est une donnée supplémentaire (en général, un nombre secret) qui est nécessaire pour actionner le verrou : sans cette clé, celui qui connaît l'algorithme ne pourra pas déchiffrer le message. »* La différence entre les systèmes RSA et AES tient, en fait, au nombre de clés utilisées. En effet, AES emploie une seule et même clé, dite "privée" (car tenue secrète), pour le codage et le décodage du message : on le qualifie de *système à clé privée*. Les interlocuteurs doivent donc s'échanger cette unique clé, d'où la vulnérabilité du système. Tandis que RSA est un *système à clé publique* ; il utilise non pas une mais deux clés distinctes : l'une publique (connue de tous) pour le codage, et l'autre secrète et propre à chaque correspondant, pour le décodage. Les risques liés au partage de la clé de décodage sont donc supprimés, d'où l'extrême sûreté de ce système.

Une seconde suffit pour le codage et le décodage

Ainsi, plutôt que d'essayer d'inventer un nouveau système cryptographique – il faudrait des années pour cela ! –, les chercheurs ont tout simplement choisi de combiner les systèmes AES et RSA : le plus rapide des deux (AES) servant au (dé)codage du message proprement dit (l'image numérique) ; le plus lent (RSA), mais aussi le plus sûr, servant à coder la clé secrète utilisée pour le décodage du message (*voir encadré*).

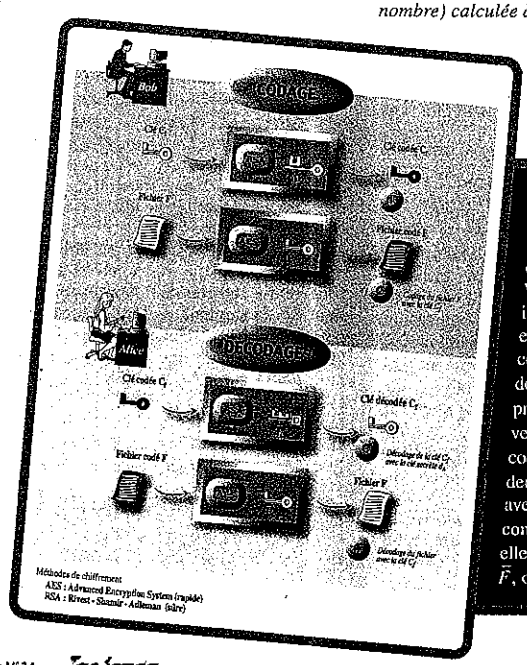
Toutefois, ce protocole ne permet pas, à lui seul, de garantir l'intégrité du document transmis. *« Pour cela, nous avons intégré au système une "fonction de hachage", c'est-à-dire un algorithme qui associe au fichier transmis une "empreinte" (un nombre) calculée à partir du contenu de ce fichier »*, précise le mathématicien.

Or c'est cette même empreinte qui sert à "fabriquer" la clé de décodage du fichier. De fait, si le fichier est altéré au cours de l'envoi, son empreinte le sera elle aussi, et la clé également. Résultat : le déchiffrage du message sera impossible. Avec ce procédé, le destinataire a donc un moyen simple et qui plus est, rapide, de vérifier l'intégrité des données reçues.

Car l'ensemble des opérations est entièrement automatisé (il suffit à l'expéditeur de fournir au programme le nom du fichier et celui du destinataire) et ne prend pas plus d'une seconde pour une image médicale de taille standard (10 mégaoctets), avec un banal ordinateur de bureau !

Il reste néanmoins à tester le système en conditions d'utilisation réelles. Pour l'heure, la méthode fonctionne efficacement avec deux correspondants. Mais qu'en est-il s'il y en a plusieurs et s'il y a un grand nombre d'images à transférer ? C'est ce à quoi devront répondre les chercheurs lyonnais et grenoblois dans les mois qui viennent. ●

(1) Université Lyon 1
Institut Girard Desargues
(UMR 5028 CNRS/UCBL)
Bât. Jean-Braconnier
69622 Villeurbanne Cedex



Bob parle à Alice

Le protocole de cryptographie conçu par les chercheurs pour la télétransmission d'images médicales allie la sûreté de la méthode RSA avec la rapidité de la méthode AES. Voici son principe de fonctionnement pour deux interlocuteurs, Bob et Alice. Supposons que Bob veuille envoyer un fichier F à Alice. Celle-ci détient une clé de codage c_A publique, donc connue de Bob, et une clé de décodage d_A qui reste secrète. Bob commence par envoyer un premier message très court, dont le contenu est $\overline{c_f}$, qui est la version cryptée, avec la méthode RSA et la clé c_A, de la clé de codage du fichier c_f (choisie par Bob) ❶. Puis il envoie un deuxième message plus long, qui correspond au fichier $\overline{F}$, codé avec la méthode AES et la clé c_f ❷. Pour lire le message, Alice commence par décoder la clé $\overline{c_f}$ avec RSA et sa clé secrète d_A : elle obtient c_f ❸. Puis elle utilise AES et la clé c_f pour décoder $\overline{F}$, obtenant ainsi le fichier original F ❹.