La cryptographie, un art toujours perfectible

- Informatique - Sécurité Informatique -

Date de mise en ligne : mardi 18 janvier 2011

Spyworld Actu

A l'ère du tout numérique, le codage des informations est devenu vital. Pour les gouvernements comme pour chaque individu.

La cryptographie est un mélange de concepts mathématiques complexes et d'astuce. C'est aussi une course-poursuite perpétuelle entre crypteurs et décrypteurs, encore accélérée par l'augmentation continue de la puissance des ordinateurs. Dans ce contexte, il est souvent difficile de distinguer les gentils des méchants ou de dire de quel côté se situent les services de renseignements des Etats - démocratiques ou pas.

La généralisation de la numérisation des données et des communications a fait exploser la demande en cryptographie. "Avec l'affaire WikiLeaks, les gens vont être bien plus sensibles à la problématique de la sécurité des informations", commente Grégoire Ribordy, directeur de la société de cryptographie genevoise ID Quantique. "Envoyer un e-mail, c'est un peu comme envoyer une carte postale. On y met pourtant du contenu personnel, ou même des contrats de travail, que l'on ne coucherait jamais sur carte postale. Crypter revient à utiliser une enveloppe."

L'art du secret est pourtant ancien. César, par exemple, se servait d'un code très simple : il décalait chaque caractère du message à transmettre d'un nombre déterminé de lettres dans l'alphabet. L'illettrisme était assez élevé à l'époque pour que cela suffise. Les efforts fournis pendant la Seconde Guerre mondiale pour décrypter les messages ennemis ont donné naissance aux premiers ordinateurs.

Menaces sur les protections

Il y a deux grandes catégories de méthodes de chiffrement. Les systèmes à clé secrète, ou symétrique, impliquent un échange confidentiel initial entre les deux personnes qui souhaitent partager des données - comme le nombre de lettres de décalage dans le code de César. Ils sont utilisés, par exemple, dans la téléphonie mobile. Les échanges entre le portable et l'antenne de réception sont codés au moyen d'une clé secrète, inscrite dans la carte SIM de l'appareil et dans le serveur de l'opérateur, que l'antenne sollicite au début de chaque communication. L'inconvénient de ce type de système est que l'échange initial de clés peut être intercepté. En outre, si l'on souhaite communiquer avec beaucoup de personnes, il est peu pratique de devoir transmettre une clé à chacune d'entre elles. C'est là où les systèmes à clé publique, ou asymétrique, sont avantageux. Il existe une clé connue avec laquelle quiconque peut crypter un message. Les premiers algorithmes permettant ce type de cryptage - les algorithmes RSA - ont été inventés dans les années 1970. "On sait aujourd'hui que l'armée anglaise avait déjà mis au point ce système, mais elle l'a gardé secret et elle est passée à côté de son exploitation commerciale", raconte Nicolas Gisin, physicien à l'université de Genève et membre fondateur d'ID Quantique. Avec la progression de la puissance des ordinateurs, les différents niveaux de sécurité RSA (correspondant à diverses tailles de clés) sont toutefois en train de tomber les uns après les autres. Des clés de plus en plus longues et coûteuses en temps de calcul lors du cryptage sont nécessaires. On est donc en train de passer à des algorithmes à courbes elliptiques, des objets mathématiques qui redéfinissent les calculs d'addition et permettent d'utiliser des clés plus courtes.

S'il faut néanmoins encore beaucoup de temps et d'énergie pour venir à bout de ces codes, il se peut qu'un jour un Champollion [célèbre déchiffreur de hiéroglyphes égyptiens ayant vécu au XIXe siècle] moderne trouve un moyen de les décrypter sur un PC ordinaire, fait valoir Nicolas Gisin. "Ce serait une catastrophe pour notre société. Tout argent électronique perdrait immédiatement sa valeur", commente-t-il, avant d'ajouter que l'Agence de sécurité nationale américaine (NSA) y est peut-être déjà parvenue.

Les ordinateurs quantiques sont encore au stade embryonnaire, mais ils font peser une menace réelle sur les systèmes à clé publique. Ils devraient en effet ne faire qu'une bouchée de ce type de cryptage. Sans compter qu'avec une puissance de calcul immense on peut toujours tenter une attaque en force : c'est-à-dire en essayant successivement toutes les clés possibles. Grégoire Ribordy souligne que des petits malins sont peut-être déjà en train de stocker des données cryptées en attendant qu'apparaisse la technologie nécessaire pour les lire.

Pour l'instant, beaucoup de systèmes de cryptage utilisent "le meilleur des deux mondes" : une clé publique qui permet d'échanger une clé secrète. Le traitement des données est ainsi mille fois plus rapide. L'e-banking, par exemple, fonctionne selon ce principe. C'est l'un des rares domaines, avec la téléphonie mobile, le Wi-Fi, le Bluetooth, les bancomats ou encore la télévision cryptée, où les particuliers utilisent le cryptage. Ainsi, les e-mails demeurent la plupart du temps non cryptés. "C'est aussi le cas dans beaucoup d'entreprises sérieuses, observe Nicolas Gisin. Cela commence toutefois à changer." Les sociétés codent surtout les échanges entre les réseaux externes et leur réseau interne, ainsi que les "backups", les données qui sont sauvegardées.

Quant aux gouvernements, il est difficile de savoir ce qu'ils cryptent et comment. "Ils se servent d'algorithmes dits 'propriétaires' : en bref, on ne sait pas ce qu'ils utilisent, précise Grégoire Ribordy. C'est censé ajouter un degré de sécurité. Mais, comme cela réduit le nombre de personnes capables d'analyser les failles de ces systèmes, cela les rend aussi plus vulnérables..." Sauf pour les Etats qui ont les moyens de se payer une armée de hackers pour les tester.

Un matériel de guerre

Il existe un code dont l'inviolabilité a été prouvée : l'algorithme du masque jetable. Il est toutefois très peu pratique. La clé doit être totalement aléatoire et de la même longueur que le message. En outre, elle ne peut être utilisée qu'une fois. "C'est inapplicable, sauf pour le téléphone rouge entre Washington et Moscou, pour autant qu'il existe encore", observe Serge Vaudenay, directeur du laboratoire de sécurité et cryptographie de l'Ecole polytechnique fédérale de Lausanne.

Les Etats surveillent de près tout ce qui touche à la cryptographie. Considérant qu'il s'agit de matériel de guerre, plusieurs gouvernements - dont ceux de la France et des Etats-Unis - ont longtemps été très restrictifs en matière d'exportation, d'importation et même d'utilisation. Les agences de renseignements ont accès à une bonne technologie cryptographique. De même que les trafiquants d'armes ou de drogue. Mais les gens ordinaires et les organisations politiques de base n'ont pour la plupart pas eu accès à une technologie cryptographique de "qualité militaire" abordable.

"A une époque, la version américaine d'Internet Explorer avait une clé de sécurité de 128 bits, tandis que la version internationale en avait une de 40 bits, explique Grégoire Ribordy. Certains disent que si cela n'est plus le cas, c'est que c'était devenu incontrôlable. D'autres, plus cyniques, estiment que c'est parce que les services de renseignements peuvent aujourd'hui décrypter des clés plus longues." Depuis, les choses se sont simplifiées avec la signature d'accords internationaux.

La France, en tout cas jusqu'à une époque récente, demeurait toutefois ta-tillonne sur les importations, précise le spécialiste. Soit pour des questions de surveillance interne, soit pour s'assurer de la sécurité de son industrie. L'Hexagone a en effet été mêlé à plusieurs affaires d'espionnage industriel. Les autorités n'ont, en outre, libéralisé l'utilisation de la cryptographie qu'en 2004, tandis que, dans d'autres pays comme la Chine, celle-ci est toujours soumise à autorisation. Ceux qui détiennent l'art du secret ne tiennent pas à le partager.

Post-scriptum :

http://www.courrierinternational.co...