Les enjeux de la cryptologie

Elle a connu ses premiers balbutiements il y a plusieurs millénaires. Pourtant la cryptologie est une science très jeune qui a véritablement éclos avec l'avènement de l'informatique et la généralisation des télécommunications. Longtemps fermée, réservée aux militaires et à la diplomatie, elle touche tout le monde depuis l'explosion d'Internet. Quels sont ses enjeux techniques et sociétaux, ses moyens et ses perspectives ? Réponses à travers les travaux de l'équipe de l'ENS/CNRS.

Qu'y a-t-il de commun entre la carte SIM de votre téléphone, une carte bancaire, vos sites Internet préférés d'emplettes ? Un mot les relie : cryptologie.

En effet, dans la société de l'information, l'usage de la cryptologie s'est banalisé. Téléphones mobiles, cartes bleues, titres de transports, cartes vitales, décodeurs, Internet, on ne compte plus les objets de la vie courante qui incorporent des mécanismes de sécurité. Des algorithmes cryptographiques assurent par exemple que personne ne peut téléphoner à vos frais, intercepter un numéro de carte de paiement sur la Toile, accéder aux données confidentielles d'une carte vitale, etc.

Jadis restreinte aux usages diplomatiques et militaires, la cryptologie est maintenant devenue une discipline scientifique à part entière dont les applications sont si vastes aujourd'hui qu'il est difficile de définir *a priori* ce qui en relève. Initialement, elle avait pour objet l'étude des méthodes permettant d'assurer les services d'intégrité, d'authenticité et de confidentialité dans les systèmes d'information et de communication. Reposant sur l'utilisation de clés, elle recouvre désormais l'ensemble des procédés informatiques qui doivent résister à des adversaires ne respectant pas les « règles du jeu ».

Qu'est-ce que la cryptologie ?

La cryptologie a pour essence l'art de cacher une information au sein d'un message chiffré. C'est un art très ancien : les premiers codes secrets remontent à l'antiquité.

Elle se divise en deux branches :

- la **cryptographie** concerne la conception de mécanismes destinés à garantir les notions de sécurité.
- la **cryptanalyse** consiste à tenter d'attaquer un système cryptographique, notamment pour en étudier le niveau de sécurité effectif.

Elle doit répondre à trois enjeux :

- Un service d'intégrité pour garantir que le contenu d'une communication ou d'un fichier n'a pas été modifié de façon malveillante.
- Un service d'authenticité pour s'assurer de l'identité d'une entité donnée ou l'origine d'une communication ou d'un fichier. Lorsqu'il s'agit d'un fichier et que l'entité qui l'a créé est la seule à avoir pu apporter la garantie d'authenticité, il s'agit de la non-répudiation. Ce service est réalisé par une **signature numérique**, qui a une valeur juridique depuis la loi du 20 mars 2000.
- Un service de confidentialité pour garantir que le contenu d'une communication ou d'un fichier n'est pas accessible aux tiers. Des services de confidentialité sont offerts dans de nombreux contextes, notamment en téléphonie mobile, en télévision à péage et dans les navigateurs Internet par l'intermédiaire du protocole SSL/TLS.

Les principaux concepts

Jusqu'à la fin du XIX^{e} siècle, la plupart des techniques cryptographiques faisaient reposer leur sécurité sur le secret même de l' « algorithme » et n'étaient pas adaptées à un usage au sein d'un grand groupe de personnes. C'est pourquoi on a ensuite personnalisé le mécanisme avec une information de petite taille, appelée **clé secrète,** commune à l'émetteur et au destinataire. Puis ces méthodes de **cryptographie symétrique** à clé secrète se sont améliorées et complexifiées avec l'arrivée de l'électronique et de l'informatique.

La cryptologie a connu une mutation importante, au moment même où Internet se préparait, avec l'apparition de la cryptographie dite à **clé publique**, qui a ouvert un domaine de recherche très riche avec tous les problèmes pratiques de sécurité : authentification, confidentialité, commerce, vote, enchères et toutes autres formes d'échange de données nécessitant intégrité, non-répudiation ou anonymat. En effet en 1976, deux scientifiques, Whitfield Diffie et Martin Hellman ont imaginé de rendre tout le processus de chiffrement entièrement public, non seulement les algorithmes, mais encore une clé spécifique au destinataire, la clé publique. Seule la clé de déchiffrement doit rester secrète. Ainsi, chaque individu possède un couple de clés, l'une publique qui sert à ses interlocuteurs pour chiffrer des messages, l'autre secrète qui lui sert à déchiffrer les messages reçus, chiffrés à l'aide de sa clé publique. Cette **cryptographie asymétrique** permet également de concevoir des schémas de signature. Le déchiffrement, accessible uniquement à qui connaît la clé secrète, devient l'algorithme de signature. En revanche, l'opération réciproque de chiffrement étant accessible à tous devient l'algorithme de vérification qui doit conduire au message initial. La non-répudiation peut alors être garantie.

Ce principe a été mis en œuvre dès 1978 dans l'algorithme **RSA** inventé par Ron Rivest, Adi Shamir et Leonard Adleman. Dans le RSA, la sécurité est liée à la difficulté de calculer les facteurs premiers d'un nombre entier de plusieurs centaines de chiffres au moins : le record – qui date de mai 2005 –

est de 200 chiffres. De plus, en matière d'authenticité, une signature RSA est vérifiable avec la seule clé publique tandis que sa création nécessite la clé secrète de son titulaire, ce qui garantit la non-répudiation.

Cette cryptographie à clé publique apporte des solutions pour la non-répudiation d'une transaction électronique et sa confidentialité, ou l'anonymat d'un vote. Mais attention : l'efficacité du système repose sur la « confiance », qui elle-même doit s'appuyer sur la gestion des clés publiques par une autorité de certification habilitée à délivrer et à signer des clés (banque, administration des impôts, entreprise, ministère, etc...). De plus, la sécurité des mécanismes n'est pas inconditionnelle, mais dépend des hypothèses mathématiques qu'il faut identifier clairement afin d'évaluer leur validité. Il s'agit des deux problèmes majeurs posés à la fois aux pouvoirs publics et à la communauté scientifique pour que la cryptographie puisse assurer la protection des libertés individuelles, dans un monde envahi par le numérique, sans risquer d'être détournée à des fins malhonnêtes.

Dans les trente dernières années, la recherche en cryptologie a connu un considérable développement, se concentrant sur la conception et l'évaluation d'algorithmes symétriques et à clé publique. Cette recherche s'est accompagnée d'un effort de normalisation exceptionnellement enraciné dans les recherches les plus récentes et fondé sur un rapprochement entre la recherche académique et le monde industriel.

La recherche française en pointe

Sans revenir sur tous les travaux qui ont été réalisés, évoquons ici deux axes de recherche prometteurs apparus dans les dernières années et étudiés au laboratoire LIENS, dirigé par Jacques Stern.

La sécurité prouvée

Le plus grand progrès qu'ait connu la cryptographie asymétrique depuis son invention est la méthodologie de la sécurité prouvée, ou **preuve de sécurité**, qui complète la cryptanalyse par de véritables preuves d'absence de failles. Il s'agit dans un premier temps de modéliser la notion même de sécurité, puis de construire des cryptosystèmes prouvés sûrs dans ce modèle, sous des hypothèses mathématiques précises et plausibles.

La sécurité prouvée met en œuvre une approche réductionniste : on traduit la sécurité en une hypothèse sur la difficulté de résoudre par le calcul un problème bien connu et bien défini, comme la factorisation ou le logarithme discret. Si l'hypothèse est satisfaite, le système est sûr. Le principal avantage de cette approche est que l'on peut clairement identifier l'hypothèse sur laquelle repose la sécurité, le principal inconvénient étant que l'on n'obtient pas de preuve absolue : on a juste remplacé un énoncé complexe par une hypothèse plus claire. Reste à suivre les progrès dans la résolution des problèmes supposés difficiles et à dimensionner la taille des clés en conséquence.

Malheureusement, dans la plupart des cryptosystèmes asymétriques pratiques, notamment ceux qui sont normalisés, la traduction de l'énoncé complexe en une hypothèse plus claire n'est pas nécessairement pertinente pour les tailles de clés courantes. Pour contourner ce problème, les chercheurs ont opéré une idéalisation des fonctions d'intégrité dites aussi de « hachage », connue sous le nom de modèle de « l'oracle aléatoire ». La méthode revient à faire l'hypothèse supplémentaire que l'attaquant n'exploitera pas les spécificités intrinsèques des fonctions de hachage utilisées. Dans ce modèle idéal, de nombreux systèmes cryptographiques efficaces ont pu être prouvés sûrs, sous des hypothèses calculatoires plausibles.

La cryptographie fondée sur l'identité

Un autre grand problème de la cryptographie asymétrique est la gestion des clefs publiques, et plus précisément la façon de garantir l'authenticité de ces dernières. Dans le cas d'Internet, ce problème est actuellement résolu à l'aide de certificats, bien connus des habitués des sites marchands. La cryptographie asymétrique fondée sur l'identité propose une solution alternative en permettant aux clefs publiques d'être directement reliées à l'identité des utilisateurs : toute chaîne de caractères, par exemple une adresse électronique, est une clef publique potentielle.

Cela est rendu possible par l'intermédiaire d'une autorité de certification en laquelle tous les utilisateurs ont confiance : l'autorité choisit des paramètres publics, et à chaque fois qu'un utilisateur souhaite enregistrer une clef publique (de valeur arbitraire), l'utilisateur l'envoie à l'autorité, qui lui retourne la clef secrète correspondante. Contrairement à ce qui se passe dans les infrastructures de clés publiques traditionnelles, l'autorité a connaissance de toutes les clés secrètes.

La cryptographie à base d'identité est en plein essor, mais elle n'est donc pas sans inconvénient. De plus, elle a dû faire appel à des théories mathématiques complexes dont l'aspect algorithmique n'a pas encore fait l'objet de recherches approfondies.

Pour en savoir plus :

- Jacques Stern, *La science du secret,* Editions Odile Jacob, 1997.
- David Kahn, *La guerre des codes secrets,* Paris, InterEditions, 1980.
- *Paradigmes et enjeux de l'informatique*, sous la direction de Nicole Bidoit, Luis Farinãs del Cerro, Serge Fdida, Brigitte Vallée, Editions Lavoisier, 2005. Chapitre 6 : La cryptologie : enjeux et perspectives. Phong Q.Nguyen, Jacques Stern.
- David Pointcheval, *La cryptographie à l'aube du troisième millénaire.* Revue de l'électricité et de l'électronique. Volume 5, pages 28-34. Dossier spécial *La sécurité des systèmes d'information*, SEE, mai 2001.