

CHAPITRE 10

La cryptographie

Mireille CAMPANA

Le principe historique de la cryptographie, qui est définie comme l'art d'écrire en éléments secrets, est la dissimulation du contenu d'une information au moyen d'un procédé connu de ses seuls utilisateurs.

Elle fournit deux grands types de services :

1 / ceux liés à la *confidentialité* des informations stockées ou échangées qui s'appuient sur la mise en œuvre de procédures de chiffrement ;

2 / ceux liés à l'*authenticité* des informations : intégrité du contenu et identification sûre de l'origine, qui recourent à des mécanismes dits « de signature électronique ». La signature numérique permet également d'assurer la « non-répudiation » de l'émission d'un message.

Les années 1990 ont été marquées par l'explosion des systèmes de communication, qui ont permis le développement des échanges électroniques, tant dans le domaine industriel et bancaire que dans celui du commerce en ligne et récemment celui des relations entre les citoyens et les administrations. Si, jusqu'à présent, l'ouverture et l'« interopérabilité » des réseaux et systèmes, ainsi que leurs performances, ont été privilégiées aux dépens de la sécurité, on assiste maintenant à une prise de conscience des problèmes par les acteurs de ces nouveaux réseaux, qui ont engagé des réflexions sur la sécurité et sur la cryptographie qui en constitue une brique fondamentale.

Longtemps réservée au domaine diplomatique et militaire, s'appuyant alors sur des principes mathématiques élémentaires, la cryptographie a commencé à évoluer vers le milieu du siècle avec le début des télécommunications en intégrant essentiellement des techniques de codage de l'information ; mais il a fallu attendre les années 1970 pour qu'elle passe du secret des laboratoires militaires au domaine public, et s'institue comme une véritable science dans le domaine universitaire. Beaucoup d'articles ont alors été publiés et des conférences publiques ont été instituées. .

Des liens avec d'autres disciplines des mathématiques telles que codage et probabilités, arithmétique et géométrie algébrique, ont été établis. Cette évolution a été rendue nécessaire par le développement de l'informatique et des

télécommunications qui entraînait des besoins de protection pour tous; elle s'est accompagnée, dans certains pays, de la mise en place de législations et de réglementations qui pouvaient restreindre l'usage des procédés cryptographiques, dans le but de ne pas contrevenir aux besoins de la sécurité nationale et de la sûreté publique.

Ces législations, quand elles étaient explicites, ont pris des formes différentes, mais trois grandes tendances se sont dégagées : les pays qui n'effectuent en pratique aucun contrôle, comme l'Australie ou la Norvège ; les pays, les plus nombreux, parmi lesquels les États-Unis et la plupart des États européens, qui contrôlent uniquement l'exportation¹ des dispositifs cryptographiques et laissent la commercialisation et l'usage libres sur leur territoire ; enfin, les pays qui contrôlent l'usage et la commercialisation de ces dispositifs cryptographiques. La position américaine, qui s'appuyait sur le respect et la garantie de la protection individuelle mais aussi sur la libre entreprise, est en cours d'évolution ; même les contrôles portant sur les exportations sont actuellement remis en cause sous la pression des industriels exportateurs, et cet assouplissement sera vraisemblablement suivi par les autres pays.

Jusqu'à janvier 1999, la France a appartenu à la troisième tendance avec un système législatif et réglementaire très élaboré et fréquemment révisé, qui visait à obtenir un équilibre entre la protection des entreprises et des individus, d'une part, les obligations liées à la sécurité de l'État, d'autre part. La dernière législation (loi de réglementation des télécommunications de 1996 complétée par des décrets de 1998) mettait en place un système reposant sur un emploi libre des produits de force limitée² ou utilisant des clés qui pouvaient permettre à l'administration la récupération des données *a posteriori* dans certaines conditions.

Cet ensemble complexe de décrets et d'arrêtés était prévu non seulement pour pouvoir facilement s'adapter aux besoins du marché et aux progrès de la technologie, mais aussi pour permettre un changement de position politique sur le contrôle ; il a permis à la France de passer très rapidement, et sans avoir à légiférer, de la troisième à la deuxième tendance (dans la pratique, sinon formellement dans les textes) en relevant de 40 à 128 bits la longueur de clé des produits de cryptographie, par deux décrets simples (n^{os} 99-199 et 99-200 du 17 mars 1999). Ces décisions revenaient à accorder la liberté d'utilisation à la quasi-totalité des dispositifs cryptographiques (en particulier des produits dits

¹ Les règles applicables à l'exportation des cryptographiques qui sont considérés comme des « biens à double usage » (usage civil et usage militaire) sont définies dans le cadre des arrangements de Wassenaar de juillet 1996, plusieurs fois révisés par la suite ; ils concernent la plupart des pays industrialisés. Ces règles sont appliquées plus ou moins sévèrement selon les pays.

² Bien que les réalités techniques puissent être parfois différentes, il est souvent d'usage d'évaluer l'efficacité de la protection que procure un dispositif en fonction de la taille de sa clé. On verra la signification de ce paramètre dans la description des techniques.

« forts »). En outre, les formalités administratives sont allégées pour les utilisateurs ; elles ne pèsent plus que sur les fournisseurs qui doivent, pour commercialiser leurs produits, effectuer une déclaration auprès du SCSSI³ à laquelle est jointe un dossier technique décrivant le produit.

Une nouvelle législation est en cours d'élaboration ; elle devrait prendre en compte de nouveaux besoins apparus avec le développement du commerce électronique, comme les signatures dématérialisées.

LES TECHNIQUES

Des procédés secrets, on a évolué vers des algorithmes mathématiques connus utilisant des paramètres secrets que l'on a nommés « clés ». Actuellement, la cryptographie classique (dite symétrique ou à clé secrète) repose sur ce principe. Pour chiffrer un message, on utilise un algorithme répertorié ou correspondant à un standard⁴ s'appuyant sur un paramètre secret, la clé, qui est un *nombre* connu des différents interlocuteurs. Il est relativement facile de construire de tels algorithmes et seuls les besoins d'interopérabilité des systèmes de cryptographie limitent leur nombre. Les États-Unis, dans les années 1970, ont tenté d'imposer un algorithme, unique, baptisé DES (*Data Encryption Standard*), en insistant sur les problèmes d'interopérabilité et aussi de sécurité et d'économie. Pour cela, le département du Commerce a fait réaliser par la Société IBM un algorithme qui devait être publié, de manière à permettre son évaluation par tous, et qui devait être libre de tous droits d'usage. Plus de vingt ans après, la seule faiblesse révélée de cet algorithme est la longueur de la clé (56 bits), jugée trop courte pour les moyens de calcul actuels (6).

Même si le DES n'a jamais obtenu le statut de norme internationale, essentiellement pour des raisons politiques car certains États s'opposaient alors à la prolifération de dispositifs cryptographiques, il a été pendant des années l'algorithme employé de façon systématique dans le domaine commercial et reste aujourd'hui le plus employé. Il a quelques concurrents, essentiellement dans le domaine des produits logiciels, comme le RC4 ou IDEA, qui sont mieux adaptés à des implantations logicielles. Les applications gouvernementales utilisent pour des raisons de sécurité des algorithmes non publiés; il en va de même dans le domaine des télécommunications où les opérateurs ont en général préféré définir leurs propres normes⁵.

³ Service central de la sécurité des systèmes d'information chargé de l'application de la réglementation. Avant mars 1999, la commercialisation et l'utilisation de tout dispositif cryptographique étaient soumises à autorisation de ce service. C'est toujours le cas pour les dispositifs dont la taille des clés servant au chiffrement d'information dépasse 128 bits.

⁴ La fonction est a priori connue de tous; on verra plus loin les exceptions à cette règle.

⁵ Ces normes ne sont pas toujours publiées ; cependant, dans la mesure où elles ont vocation à être fournies aux différents constructeurs dans tous les pays, leur caractère confidentiel peut être considéré comme relatif.

Il existe deux systèmes de chiffrement.

Les systèmes de chiffrement à clé secrète, ou systèmes symétriques

Ils reposent sur le partage entre deux interlocuteurs en communication, d'une même clé secrète S qui sert à paramétrer un algorithme à la fois pour *le chiffrement d'un message et pour son déchiffrement*. La clé S doit faire l'objet d'un échange physique préalablement à toute communication. Pour le stockage de messages, le principe est le même avec un seul interlocuteur. Cette clé prend en général la forme d'un ensemble de bits de taille limitée. Un procédé, connu sous le nom d' « attaque par force brute », utilisé pour retrouver le contenu des communications, consiste à essayer toutes les clés possibles⁶. Leur nombre dépend de la taille de ces clés : pour une clé de n bits, il y a 2^n clés possibles ; la complexité d'un produit est donc bornée par la taille de cet ensemble.

En général, la clé secrète commune S n'est pas utilisée directement pour chiffrer les messages, mais pour chiffrer une autre clé K qui est un nombre tiré au hasard par l'émetteur à chaque session et qui sert comme clé secrète pour chiffrer les messages. Cette clé K chiffrée est envoyée en début de session ou de message ou, dans le cas de stockage, conservée avec le message.

Les systèmes à clé publique ou systèmes asymétriques

Les algorithmes à clé publique servent à chiffrer des messages, mais aussi à calculer des signatures numériques. Une signature numérique est une valeur qui dépend du message, considéré alors sous sa forme numérisée comme un nombre, et de l'identité du signataire, qui doit être le seul à pouvoir calculer cette signature. Un message signé est composé du message en clair et de cette signature numérique. Vérifier une signature consiste, en appliquant la fonction inverse de la signature, à retrouver le message en clair.

Chaque utilisateur possède son propre couple de clés différentes S et P :

La clé S est gardée *secrète* par son propriétaire qui l'utilise pour *déchiffrer* des messages reçus ou *signer* des messages.

⁶ La complexité de cette attaque par force brute dépend de la vitesse d'exécution de l'algorithme et de la puissance de calcul utilisée ; à titre indicatif, pour certains algorithmes courants type DES, il est possible de retrouver une clé de 40 bits en quelques heures ou dizaines d'heures de PC. Cette complexité est multipliée par un facteur 65 000 si l'on passe à 56 bits ; pour 128 bits, effectuer ce type de recherche exigerait des ressources très largement non disponibles à l'heure actuelle.

La clé P est rendue *publique*. Elle dépend de la clé S par une fonction à sens unique : la fonction est facilement calculable, mais son inversion est extrêmement difficile (on ne sait pas déduire S de P). Elle sert à quiconque pour *chiffrer* les messages destinés au propriétaire du couple de clés, ou à *vérifier* les signatures.

Pour chiffrer un message destiné à une personne A , le correspondant B applique la fonction définie par P_A , la clé publique de A . A le déchiffre avec sa clé secrète S_A qu'elle est seule à détenir.

Pour signer un message, B lui applique la fonction définie par sa clé secrète S_B pour calculer une signature. Pour vérifier cette signature, A lui applique la fonction inverse de la fonction de signature, définie par la clé publique P_B de B , ce qui lui permet de retrouver en clair le message initial. Seul B , qui détient S_B , a pu calculer cette signature.

<i>B envoie un message chiffré et/ou signé à A</i>	
B chiffre avec P_A	A déchiffre avec S_A
B signe avec S_B	A vérifie avec P_B

Comme les algorithmes à clé publique sont lents à exécuter, on chiffre toujours les messages avec des algorithmes à clé symétrique, et on utilise le dispositif à clé asymétrique pour chiffrer la clé de session générée aléatoirement, comme dans le cas des systèmes à clé secrète.

Relation entre la clé publique et son détenteur

Le problème fondamental que pose l'utilisation de la clé publique peut se définir ainsi: comment établir un lien sûr entre une clé publique P_A et son détenteur A ? Il est absolument fondamental pour l'émetteur du message de pouvoir être sûr que la clé publique qu'il utilise pour chiffrer un message, destiné à A , est bien celle de A . De la même façon, pour vérifier les messages signés par A , il faut être sûr du lien entre A et la clé publique P_A qui sert à vérifier les signatures. Les inventeurs⁷ du concept de clé publique préconisaient l'utilisation d'annuaires de clés publiques utilisant des supports non modifiables (papier ou support magnétique non « ré-inscriptible »).

Il est possible également d'utiliser des certificats créés par des *autorités de certification*, et c'est la solution retenue à l'heure actuelle. Un utilisateur A présente sa clé publique P_A à une telle autorité, qui possède elle-même un couple

⁷ Diffie et Helleman, qui ont formalisé pour la première fois en 1977 le concept de chiffrement asymétrique et proposé un schéma d'échange de clés reposant sur ce concept.

$(P_{\text{aut}}, S_{\text{aut}})$; P_{aut} , est supposée connue de tous. L'autorité vérifie l'identité de A et signe avec sa clé secrète l'ensemble constitué de l'identité et de la clé publique de A, à savoir : Certificat = Signature $S_{\text{aut}}(ID_A, P_A)$ où ID_A désigne l'identité de A.

Seule l'autorité peut calculer des certificats vérifiables avec P_{aut} en signant des ensembles identité-clé publique.

Les *certificats* peuvent être placés dans un annuaire qui ne requiert pas de sécurité particulière. Lorsque A émet un message signé avec S_A , il l'accompagne de son certificat (ou le destinataire retrouve celui-ci dans l'annuaire). Pour vérifier la signature émise par A, le destinataire B, qui dispose de la clé publique de l'autorité P_{aut} , (supposée connue de tous), peut vérifier le certificat de A, c'est-à-dire retrouver l'ensemble (ID_A, P_A) et acquérir la certitude que P_A correspond bien à A ; il utilise ensuite P_A pour vérifier la signature du message émis par A.

Le concept de clé publique a remis en cause les architectures traditionnelles d'organisation de la cryptographie. L'utilisation de schémas à clé secrète permet de définir des groupes d'utilisateurs appelés généralement réseaux qui partagent un même secret et l'utilisent pour communiquer entre eux de manière sécurisée. L'utilisation de procédés à clé publique n'implique aucun partage de secret entre les utilisateurs mais implique l'existence d'une autorité de certification appelée souvent tiers de confiance qui va forger les certificats, assurant le lien entre les identités des personnes et de leurs clés publiques.

La sécurité de tout le système dépend du niveau de sécurité offert par cette autorité, et il est fondamental que cette autorité s'assure de l'identité d'un utilisateur avant de lui délivrer un certificat. Le niveau de confiance que l'on peut accorder au certificat est directement lié au sérieux avec lequel l'autorité de certification s'est assurée de l'identité de la personne, et aussi de la sécurité de la procédure de calcul des certificats. En particulier, la protection de la clé secrète de l'autorité est particulièrement importante, puisque c'est elle qui permet de fabriquer les certificats. Elle ne doit donc pas être accessible. Il est également important de définir des durées de validité pour les certificats. Des « profils de protection » qui sont des politiques de sécurité type ont été rédigés et validés par des groupes de travail impliquant tous les acteurs concernés (organismes institutionnels, bancaires, industriels...).

Le rôle de l'autorité de certification peut ou non comprendre la génération du couple de clés. Dans le premier cas, elle peut alors servir de tiers de recouvrement ou des clés ou même du contenu en clair des messages chiffrés, c'est-à-dire que, étant également détenteur de la clé secrète, elle a la possibilité, pour certains types de dispositifs, de retrouver le contenu d'un message chiffré, par exemple pour répondre à une demande d'un juge (ce rôle avait été envisagé dans la législation mise en place en 1996).

Il est également possible d'envisager des hiérarchies d'autorités ou des croisements lorsqu'elles se certifient entre elles afin de permettre à des utilisateurs dépendant d'autorités différentes de communiquer entre eux.

LES APPLICATIONS EXISTANTES

À l'exception de quelques secteurs comme le secteur bancaire⁸ en France ou plus récemment le secteur de la Santé, la cryptographie n'est pas à l'heure actuelle largement répandue dans les applications ; les législations restrictives ont souvent été mises en cause mais il ne faut pas méconnaître les difficultés liées à la mise en œuvre. Même dans les pays où il n'y a pas de contrôle à la fourniture et à l'utilisation des produits de cryptographie comme les États-Unis, il existe bien une offre de tels produits, surtout dans le domaine de l'Internet⁹. Mais ceux-ci ne sont généralement pas massivement employés. Il existe également des actions pour définir des standards d'algorithmes (comme le DES, mais aussi son remplaçant en cours de définition, l'AES — pour *Advanced Encryption Standard*), ou plus récemment des standards de protocoles (comme *IPSEC*, norme de chiffrement au niveau IP ou *S/MIME* pour le chiffrement de la messagerie).

Mais le caractère non obligatoire et souvent non définitif de ces standards (généralement présentés sous forme de *Request for Comments* par l'IETF) rend les industriels circonspects, et les produits ne sont pas toujours disponibles.

Par ailleurs, une fois un produit choisi, les difficultés liées à l'administration de la cryptographie, en particulier à la gestion des clés secrètes ou publiques, deviennent vite considérables dès que le nombre d'utilisateurs augmente ou que l'on veut toucher des populations diverses ou dispersées. Il n'est pas non plus évident de définir des supports protégés pour stocker les clés secrètes, en dehors des cartes à microprocesseur qui ne s'adaptent d'ailleurs pas à tous les postes de travail. Enfin, s'il est possible de placer des mécanismes cryptographiques à divers niveaux (sur les liens physiques, dans le réseau ou dans les couches logicielles applicatives), ceux-ci ne sont pas forcément transparentes. La mise en place de services de chiffrement peut gêner certains

⁸ L'ensemble du secteur bancaire français regroupé au sein du GIE Cartes bancaires a mis en place des procédures de retrait et de paiement sécurisées s'appuyant sur le choix de dispositifs sécurisés (cartes à microprocesseur) et l'utilisation de protocoles cryptographiques, ce qui a permis d'obtenir un taux de fraude très largement inférieur à ceux des autres pays, tout en assurant l'interopérabilité du dispositif.

⁹ S'il est relativement facile d'intégrer des services de chiffrement pour les échanges de données, en particulier quand cette intégration se fait dans les couches logicielles, chiffrer la voix est beaucoup plus délicat, et l'offre dans ce domaine est particulièrement restreinte et coûteuse. La téléphonie sur IP permettra peut-être de régler le problème, mais l'offre n'est pas encore mûre dans ce domaine.

services d'administration du réseau, voire le fonctionnement de protocoles de communications lorsqu'il s'agit de téléphonie.

Il y a cependant des domaines où la mise en place d'une protection du contenu des informations échangées conditionne celle des applications (les récentes révélations sur le système *Échelon* ont montré la réalité des menaces liées aux interceptions sur les réseaux publics). La *confidentialité* n'est pas le seul service nécessaire : c'est le cas en particulier du commerce électronique où l'on recherche *l'authenticité* d'une transaction mais aussi des procédures dématérialisées entre le citoyen et l'État ou les organismes sociaux.

Dans le cas d'une déclaration de revenus dématérialisée, par exemple, il est indispensable de pouvoir garantir l'identité de l'émetteur et l'intégrité des données transmises. Le secteur de la Santé a été le premier à se lancer dans la mise en place d'une telle procédure à grande échelle, à savoir la transmission électronique des feuilles de soin qui a fait intervenir une multiplicité d'intervenants (ministère, caisses d'assurance maladie, Ordre des médecins). Le volume des transactions, les enjeux financiers, les problèmes liés à l'éthique et au secret médical ont induit de très fortes contraintes de sécurité sur le réseau, les logiciels applicatifs et les dispositifs (carte de professionnel de santé et carte patient). Le ministère a fait le choix d'une *architecture à clé publique* et a mis en place une infrastructure de gestion de clés très complexe, qui est la plus importante application déployée à l'heure actuelle. Ce dispositif permet également de sécuriser les transactions entre professionnels de santé.

Au-delà de ces grands déploiements, l'entreprise qui veut sécuriser son système d'information, ou les *particuliers qui désirent sécuriser* leurs données et leurs échanges, peuvent maintenant disposer de produits ergonomiques intégrés dans des logiciels grand public, comme les navigateurs, ou s'en procurer sur le Web, comme le célèbre PGP (*Pretty Good Privacy*). Ce logiciel, développé à l'origine par un chercheur américain, Phil Zimmerman, avait pour but de mettre à la disposition de chacun les sources d'un système entier de chiffrement. Il s'est enrichi au cours des années en conservant cet esprit d'ouverture (libre disponibilité des sources) que l'on retrouve dans *Linux*. Il est cependant plus adapté à un *fonctionnement de proximité* (on reconnaît les clés de ses amis et des amis de ses amis) qu'à des applications d'achat et de paiement « impulsifs » sur Internet.

Enfin, si la *cryptographie* est l'une des briques de base de la sécurité, la plus médiatisée eu égard au secret qui a longtemps dissimulé son développement et la mieux construite, puisqu'on peut l'apparenter à une branche des mathématiques, *elle ne peut à elle seule résoudre tous les problèmes de sécurité*. Quelle que soit la force d'un algorithme ou la longueur des clés employées, il peut y avoir des problèmes d'implantation (voulus ou non) dans un dispositif, qui font qu'il est possible de retrouver les informations protégées par un moyen détourné (lorsque ces « problèmes » sont volontaires, on les désigne sous le nom de *backdoors*). Une

démarche d'évaluation des produits cryptographiques, prenant en compte non seulement la complexité cryptographique mais aussi les modes d'implantation, vient de démarrer sous l'égide du Secrétariat général de la Défense nationale (SGDN), mais c'est une tâche très lourde, en raison du volume et de la complexité des logiciels.

Par ailleurs, *la cryptographie ne protège pas les systèmes*: lorsqu'un poste de travail situé sur un réseau local établit une connexion avec le monde extérieur, même si cette connexion est protégée, elle peut être utilisée depuis l'extérieur pour effectuer des intrusions sur les machines de ce réseau local, en extraire des informations ou en détruire. Il faut mettre en place des barrières (en général désignées sous le nom de *firewalls*) comportant des filtres et des antivirus. Enfin, le problème de la connexion à l'Internet d'un poste comportant sur son disque des données confidentielles, même stockées chiffrées, est extrêmement difficile à résoudre.

ANNEXE. - Exemples de logiciels de protection couramment utilisés

Jacques Roure

Commerceserver/400 - Serveur SHTTP Pour IBM AS/400, sécurisation des transactions sur Internet.

Fols-Security - Gestion d'accès d'un client aux services d'un serveur,SEMA-GROUP.

Raptor Firewall - Constitue une solution *firewall* pour réseaux *corporate*, LAN2LAN, l'interconnexion Intranet ou l'accès à Internet.

Security Box SHL - Solution de sécurité globale pour Internet Intranet Extranet, confidentialité, authentification, intégrité.

Websentry - Autorise un accès sécurisé au Web (contrôle d'accès, chiffrement), aux applications *mainframe* (*Bull*, IBM, Unix) et multimédia.

Webaccess & Webcontrol - Accès sécurisé et contrôlé aux ressources d'Internet sans y raccorder le réseau de l'entreprise.

Webcard - Contrôle des accès à Internet. Gestion des temps de connexion. Pilotage de carte à puce.