

- *Éditorial*
par **J. Illand**
- *Le chiffrement de données*
par **X. Jeannin et M.-C. Quidoz**
- *Le déchiffrement dans le temps*
par **J.-L. Archimbaud**
- *Perspectives en cryptologie*
par **J. Stern, P. Nguyen et D. Pointcheval**

éditorial

Un impératif de protection des données sensibles

Le souci de sauvegarder ou de transmettre des données « confidentielles », à l'insu des oreilles ou des regards indiscrets, est sans doute aussi ancien que la prise de conscience par l'homme de sa capacité à communiquer. La cryptologie, science des messages secrets, s'est très tôt imposée comme une réponse s'attachant, dans ses phases de mutation scientifique, à parfaire l'invulnérabilité du secret.

Il n'est pas étonnant qu'à l'ère des technologies de l'information, des processus cryptographiques soient omniprésents et souvent transparents pour l'utilisateur, jusqu'à le rendre inconscient de l'enjeu (cartes à puce, réseaux sécurisés...).

Cette conscience de l'enjeu, en l'occurrence le prix attaché à la sécurisation (intégrité et confidentialité) d'une information, reste pourtant la base de la démarche, dans sa composante individuelle (au niveau de l'utilisateur) et dans sa dimension collective (politique de sécurité de l'organisme).

Encore faut-il savoir identifier le degré de sensibilité de l'information que l'on traite, que l'on stocke ou que l'on échange et avoir, bien sûr, la volonté de la protéger...

Ce qui semble être intuitif pour les données « personnelles » (données d'identité, données familiales, bancaires...), l'est beaucoup moins pour ce qui relève de l'activité professionnelle, à l'exception sans doute des rares habitués du « confidentiel défense » ou du « secret défense ».

C'est bien souvent à l'occasion d'un incident que la prise de conscience apparaît : vol d'ordinateur portable, piratage de données conduisant à un dépôt de brevet par un concurrent indelicat, consignes supposées « discrètes » se retrouvant dévoilées à tous, mail intercepté et indument rendu public... L'angélisme étant une « vertu » largement partagée dans le monde de la recherche, toute ressemblance avec des situations réelles douloureusement vécues serait loin d'être fortuite.

Supposons malgré tout cette prise de conscience acquise (les demandes de solutions de chiffrement, souvent exprimées au sein du CNRS, montrent au moins que la voie est prise), il reste à concevoir et à proposer des parades. Il convient bien sûr qu'elles soient efficaces. Malheureusement la solidité d'un algorithme cryptographique ne suffit pas à garantir l'invulnérabilité du secret. L'implémentation de l'algorithme et les dispositions organisationnelles demeurent essentielles pour l'efficacité d'un dispositif de chiffrement. Celui-ci d'ailleurs ne peut se concevoir sans analyse du besoin et des particularités de l'organisme, sans évaluation attentive de l'offre et sans d'indispensables précautions.

Entièrement consacré au thème de la cryptologie (1), le présent bulletin de *Sécurité Informatique* insiste d'ailleurs largement sur cette dimension méthodologique et organisationnelle. Celle-ci reste indispensable pour tirer le meilleur profit des acquis scientifiques enregistrés ces dernières décennies ou attendus des recherches en cours en mathématique et informatique.

Joseph Illand

Fonctionnaire de Sécurité de Défense

1. On pourra également se référer au bulletin n° 24 consacré en avril 1999 au même thème (<http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num24.pdf>).

■ Des recherches en amont de la cryptologie à l'honneur : Alain Aspect, médaille d'or 2005 du CNRS

La médaille d'or 2005 du CNRS a été décernée au physicien Alain Aspect, directeur de recherche au CNRS (Institut Charles Fabry - Institut d'optique d'Orsay/CNRS/université Paris-11) et professeur à l'École polytechnique, membre de l'Académie des sciences, pour ses recherches dans le domaine de l'optique quantique et de la physique atomique, avec des débouchés possibles notamment en cryptographie quantique.

Pour en savoir plus <http://www2.cnrs.fr/presse/communiquer/781.htm>

Le chiffrement de données sur les postes individuels

par **Xavier Jeannin et Marie-Claude Quidoz**
(CNRS/UREC)

La divulgation de données telles que des résultats de recherche confidentiels, des réalisations en phase d'industrialisation, des préparations de dépôts de brevets et des enquêtes médicales peut être catastrophique pour un organisme comme le CNRS. Par conséquent, de même qu'on utilise le chiffrement pour sécuriser les communications sur le réseau, il est conseillé d'utiliser le chiffrement pour protéger les données face aux risques de piratage et de vol de machine.

Chiffrer les données recouvre deux aspects : chiffrer toutes les données d'une organisation ou chiffrer les données de certains postes de travail. Dans cet article, nous nous sommes intéressés uniquement aux postes individuels et aux postes nomades. Théoriquement, aucune donnée confidentielle ne devrait se trouver sur ces derniers mais ce n'est pas le cas. Le développement de l'informatique et l'augmentation des vols des postes de travail qui l'accompagne posent le problème de la protection des informations présentes sur ces machines.

L'usage de logiciels de chiffrement peut engager juridiquement l'organisme ; il peut entraîner l'impossibilité de récupérer des données. Il doit certes intégrer les besoins des utilisateurs mais aussi la ... suite page 2 ➔

politique de sécurité informatique de l'organisme. Il n'est donc pas souhaitable de laisser l'utilisateur faire seul son choix.

Le présent article est issu d'une étude effectuée pour le CNRS qui s'appuie en particulier sur des travaux réalisés par l'INRIA que nous tenons à remercier. Il se propose, en partant d'une analyse des grandes fonctionnalités et des utilisations possibles des produits, de réfléchir aux procédures de déploiement pour arriver à des éléments de recommandation. Nous nous sommes volontairement limités dans cet article à l'exposé des principes sans présenter les résultats de l'analyse comparative des logiciels de chiffrement [1] qui a été réalisée pour le CNRS.

Les fonctionnalités disponibles

Les fonctionnalités proposées couramment correspondent aux principaux besoins des utilisateurs.

■ Le chiffrement par fichier

Chaque fichier est chiffré individuellement. Cette méthode permet de chiffrer un fichier où il est, sans le déplacer. Cette méthode a l'avantage de conserver le chiffrement lors d'un déplacement du fichier sur l'ordinateur, mais elle a l'inconvénient de devenir rapidement fastidieuse dès que le nombre de fichiers à chiffrer augmente. De plus, les fichiers temporaires sont difficilement chiffrables, ce qui peut constituer une vulnérabilité.

■ Le chiffrement dans un conteneur

Il consiste à créer un conteneur (fichier ou partition) à l'intérieur duquel tout ce qui est introduit est chiffré et tout ce qui est lu ou extrait est déchiffré (à noter qu'il est possible de travailler directement sur les fichiers chiffrés). Cette solution a l'avantage de permettre la «localisation» des fichiers chiffrés mais a l'inconvénient principal de nécessiter la création d'un conteneur avec toutes ses contraintes (réorganisation du disque dur, définition d'une taille fixe, sauvegarde incrémentale alourdie voire impossible...)

■ Le chiffrement par répertoire, voire du poste complet

Plus souple que le conteneur (pas de réorganisation nécessaire), le chiffrement par répertoire est transparent ; tout ce qui est introduit dans le répertoire est chiffré, et tout ce qui est lu ou extrait est déchiffré. Avec ce type de chiffrement, la taille de l'espace chiffré peut varier, le chiffrement se faisant fichier par fichier. Le chiffrement du poste complet est l'une des extensions du chiffrement par répertoire. Dans ce cas, le logiciel possède une liste des fichiers du système qu'il ne faut pas chiffrer, et est ainsi capable de chiffrer tout un poste, assurant ainsi une sécurité plus complète. Le chiffrement par répertoire présente aussi l'avantage de permettre de chiffrer facilement les fichiers et répertoires temporaires générés dans le système lors de l'utilisation des données.

■ Le chiffrement des données en vue de leur transmission à un correspondant via un logiciel de courrier électronique, de transfert de fichiers, etc.

Lors de collaboration entre des personnes sur des sujets sensibles, il est conseillé de chiffrer les données avant de les échanger (même si les communications sont déjà sécurisées). Le principe est un peu différent de celui utilisé pour le chiffrement du poste de travail. Ce n'est pas le fichier chiffré sur son disque qui est envoyé mais une version du fichier chiffrée spécialement pour le destinataire. Pour ce faire, avant l'envoi, l'expéditeur indique une liste de correspondants habilités à déchiffrer. Le destinataire ne doit pas obligatoirement posséder un logiciel «complet» pour déchiffrer, des modules gratuits sont fournis à cet effet. Dans ce cas le fichier est chiffré pour la transmission et non pour assurer la conservation chiffrée du fichier.

Extensions

En fonction du degré de confidentialité des données, d'autres fonctionnalités sont à considérer :

■ Le chiffrement de la partition de swap

Le système d'exploitation peut être conduit à copier les données dans la zone de swap, il est nécessaire de chiffrer cette dernière.

■ L'effacement sécurisé des données

Les logiciels fournissent des «poubelles broyeuses» qui assurent, par réécritures successives, l'impossibilité de récupérer les données sur le disque dur.

Méthodes d'exploitation et de déploiement

Différentes options sont à considérer avant d'envisager le déploiement :

■ Les clés d'accès


Pour chiffrer les données, la solution la plus classique consiste à utiliser une clé symétrique ; cette clé étant protégée par un simple mot de passe dans les solutions peu évoluées ou par une clé asymétrique (clé publique/clé privée) dans les solutions évoluées ; la clé asymétrique peut être distribuée dans le cadre d'une Infrastructure de Gestion de Clés (IGC/PKI) ou indépendamment. En tout état de cause, la distribution des clés d'accès doit être compatible avec les procédures de recouvrement définies.

Un point très important dans l'utilisation au cours du temps du chiffrement concerne le renouvellement des clés (rotation, perte ou vol de clé) : le logiciel doit pouvoir prendre en compte facilement une modification de la liste des clés d'accès, sous peine d'une gestion fastidieuse par l'utilisateur.

■ L'utilisation d'un support externe pour stocker les clés (carte à puce, token cryptographique)

L'utilisation d'un token cryptographique améliore considérablement la sécurité. De la taille d'une clé USB mémoire, facile à transporter, sa déconnexion de la machine interdit l'accès aux données ; son usage est un bon complément au chiffrement de données.

■ Le recouvrement des données

Le but de la procédure de recouvrement est de permettre la restitution des données en clair et  suite page 3

1. Logiciels de chiffrement de fichiers sur les postes personnels : fonctionnalités, critères d'évaluation et tests, X. Jeannin M.C. Quido, <https://www.urec.cnrs.fr/securite/corressecu/evaluation-produit-chiffrement.pdf>

non pas la restitution des clés d'accès ou de chiffrement. Cette restitution doit être organisée afin de pouvoir répondre aux demandes juridiques, mais aussi aux pertes de clés.

Pour réaliser le recouvrement, un séquestre du secret utilisé doit être défini. Beaucoup de produits évolués proposent, pour réaliser le recouvrement, de permettre le déchiffrement des données par plusieurs clés (la clé de l'utilisateur et les clés des responsables du recouvrement), un séquestre d'un nombre réduit de clés peut être mis en place (uniquement celles des responsables du recouvrement). Ainsi si l'utilisateur perd sa clé, d'autres personnes de confiance pourront déchiffrer ses données.

Il est primordial de définir, au niveau local, qui aura la possibilité de lire les données et qui sera en charge de sauvegarder les clés des responsables du recouvrement, l'utilisateur ayant connaissance de ces responsables. Cette organisation pourra être complétée par une procédure au niveau de l'organisme. Le recouvrement est aussi lié à la sauvegarde et à l'organisation des données; la politique de sécurité de l'organisme devra définir les éléments permettant de gérer le recouvrement.

■ La méthode de déploiement d'un logiciel de chiffrement

Chaque logiciel définit sa méthode de déploiement. Selon le mode d'administration des machines et les options définies précédemment, il faut définir les règles de déploiement et en informer les utilisateurs. Ce point relève également de la politique de sécurité.

■ La sauvegarde des données par rapport au chiffrement

La sauvegarde est un point très important de la gestion des données; la sauvegarde chiffrée augmente la confidentialité des données. Néanmoins si la sauvegarde est faite de manière chiffrée, la restauration nécessite des éléments provenant de différentes sources: les données chiffrées issues de la restauration fournies par l'administrateur système et la clé d'accès qui doit être fournie par l'utilisateur. Les procédures de restauration et les responsabilités au niveau local, tant en matière d'accès aux données en clair qu'en matière de

fourniture des éléments concourant à la restauration, doivent être bien établies.

Critères pour l'utilisateur

La facilité d'utilisation est primordiale pour l'adoption du produit par l'utilisateur final. Pour cela, il faut privilégier les critères suivants:

■ **L'ergonomie et la facilité d'installation:** le gain de sécurité n'apportant à l'utilisateur aucune fonctionnalité tangible, les contraintes doivent être minimales.

■ **La transparence:** le chiffrement doit pouvoir être automatique sans sollicitation intensive de l'utilisateur.

■ **L'identification simple:** l'utilisateur doit identifier facilement les données chiffrées pour pouvoir prendre des mesures spécifiques comme la sauvegarde, le recouvrement, etc.

Recommandations et précautions d'utilisation

Le choix d'un logiciel de chiffrement de postes personnels doit tenir compte des besoins spécifiques des utilisateurs. Pour un poste nomade, où il est important de protéger tout l'environnement, la meilleure solution est de s'orienter vers un logiciel de chiffrement de répertoire. Si le besoin se limite à sécuriser quelques documents, le chiffrement par conteneur ou par fichier peut être une bonne solution.

Au sein d'un organisme, le déploiement d'un logiciel de chiffrement nécessite une étude préalable intégrant les particularités et l'environnement de l'organisme. Nous proposons notamment de prendre en compte les points suivants:

■ Sur le plan technique

- Le chiffrement des répertoires temporaires.
- La protection par l'antivirus du poste, au moins en mode non automatique.
- La mise en place d'une procédure pour la sauvegarde des données chiffrées et leur restauration.
- Le renouvellement simple des clés d'accès.

- La procédure de recouvrement des données qui doit être efficace et légale.
- La robustesse des algorithmes cryptographiques.

■ **Sur le plan organisationnel,** il faut précisément définir

- Les données à chiffrer.
- La procédure de distribution et de renouvellement des clés.
- L'organisation du recouvrement et du séquestre des clés.
- Les responsabilités précises vis-à-vis de la sauvegarde.
- Une information des utilisateurs avec des recommandations.

Malgré tout, certaines opérations ne peuvent pas être sécurisées. Par exemple, l'utilisateur doit être conscient que l'impression d'un document entraîne une perte de confidentialité. De même, il ne faut pas utiliser le mode mise en veille mais plutôt arrêter sa machine.

En conclusion

Le chiffrement de données contribue à la sécurité de l'information à caractère sensible. Au vu des risques encourus importants (divulcation de documents électroniques confidentiels), il est devenu une parade à recommander.

Le chiffrement intègre plusieurs aspects: juridique, technique mais surtout organisationnel. Sa mise en œuvre dans un organisme tel que le CNRS pose aussi de nombreuses questions: les certificats CNRS seront-ils utilisables? Faut-il créer des certificats spécifiques à durée de validité plus longue pour le recouvrement? À qui les distribuer et sous quelle forme (token cryptographique)? Faut-il assurer un séquestre des clés?

Les choix étant multiples, il apparaît nécessaire, sur la base d'une analyse préalable, de définir une politique de chiffrement qui soit elle-même partie prenante de la politique de sécurité des systèmes d'information de l'organisme (PSSI).

Le déchiffrement des documents électroniques dans le temps : un problème à anticiper

Jean-Luc Archimbaud

Directeur de l'UREC (Unité Réseaux du CNRS)

Le CNRS dispose d'une Infrastructure de Gestion de Clés, IGC, et distribue des certificats électroniques aux personnels de ses laboratoires pour l'authentification et la signature (<http://www.urec.cnrs.fr/rubrique36.html>). Mais ils peuvent être utilisés pour chiffrer des courriers électroniques confidentiels avec les outils de messagerie standard. Un utilisateur a récemment relaté la mésaventure suivante :

«Un correspondant m'avait envoyé un message chiffré. Deux jours après je reçois un avis de renouvellement de mon certificat. Je charge le nouveau et supprime l'ancien de mon logiciel de messagerie : depuis je ne peux plus lire mon ancien message (chiffré).»

Ce problème est réel. Lorsqu'un utilisateur reçoit un courrier chiffré il ne peut être déchiffré qu'avec sa clé privée. Celle-ci est associée à un certificat électronique (qui contient la clé publique). Avec la procédure pour délivrer des certificats au CNRS, la clé privée est générée et stockée sur le poste de l'utilisateur par le navigateur utilisé lors de la demande de certificat. Quand un utilisateur renouvelle son certificat il y a création d'un nouveau couple de clés publique et privée, sans lien avec les précédentes. Si l'utilisateur supprime l'ancien certificat dans son navigateur, la clé privée associée est effacée. Cela explique le problème rencontré. L'IGC CNRS n'a pas connaissance des clés privées (le séquestre de ces clés n'est actuellement pas assuré). Seul l'utilisateur peut et doit veiller à gérer ses clés privées dans le temps. Cette anecdote met en exergue un problème théorique délicat : la gestion des documents électroniques chiffrés dans le temps, dans le cas présent celui engendré par la durée de vie des clés.

À chaque création de certificat CNRS, il faut sauvegarder (exporter) celui-ci dans un format qui contient le certificat et la clé privée associée, PKCS12 par exemple, et le ranger en lieu sûr. Si l'utilisateur avait fait cette sauvegarde, il aurait pu retrouver son ancienne clé privée et déchiffrer son courrier.

Les certificats CNRS ont été conçus pour le contrôle d'accès et la signature. Cette dernière utilisation impose d'ailleurs que seul l'utilisateur doit posséder sa clé privée, d'où le choix de ne pas faire un séquestre de ces clés.

Néanmoins on peut, avec les certificats CNRS, chiffrer les échanges de messages électroniques qui demandent une transmission confidentielle. À la réception, il est recommandé de copier le message sur le disque, ce qui le déchiffrera. Le problème ci-dessus disparaît et la confidentialité dans le transport est assurée. Si l'utilisateur souhaite conserver une version

chiffrée, il utilisera un autre logiciel (cf. ci-après) pour le «rechiffrer».

Il est vrai qu'en conservant un mail chiffré dans sa boîte aux lettres on assure un stockage de document sous forme chiffré. Mais si les logiciels de messagerie permettent un transport confidentiel, ils n'ont pas toutes les fonctions nécessaires pour éviter les mésaventures comme celle relatée. Il faut utiliser des logiciels spécifiques de chiffrement de poste de travail, présentés dans un autre article de ce numéro, qui permettent généralement :

- De garder l'équivalent d'un « historique » des clés, suivant un principe plus simple. Les documents sont chiffrés avec une clé symétrique aléatoire. Cette clé est elle-même chiffrée avec la clé publique liée au certificat et conservée ainsi. Pour déchiffrer un document le logiciel procède en deux temps : il déchiffre la clé symétrique avec la clé privée liée

au certificat puis utilise cette clé symétrique pour déchiffrer le document. Lorsque l'utilisateur change de certificat, le logiciel «rechiffre» la même clé symétrique avec la nouvelle clé publique. Ainsi il peut déchiffrer les données antérieures, la clé symétrique ayant conservé sa valeur.

- De déchiffrer les données avec plusieurs possibilités : c'est la fonction de recouvrement. Le principe est de chiffrer la clé symétrique ci-dessus avec la clé publique de l'utilisateur mais aussi avec la clé d'une personne de confiance (administrateur système ou réseau ou directeur de laboratoire...) ou d'une clé dédiée à cette fonction. Ainsi les documents pourront être déchiffrés par deux méthodes.

- D'effectuer une sauvegarde en clair des documents chiffrés.

Sans ces mécanismes, il est difficile d'assurer un service fiable de chiffrement. Mais cela ne veut pas dire qu'ils soient simples à mettre en pratique. Il reste à définir les différentes procédures (installation et configuration du produit, sauvegardes, recouvrement, restauration...), les acteurs et leurs droits... sans oublier qu'il faut assurer le séquestre de certaines clés obligatoires pour recouvrer l'ensemble des documents chiffrés en cas de perte des clés utilisateurs.

Cet article s'est focalisé sur la durée de vie des clés mais plus globalement d'autres aléas sont à prendre en compte pour garantir la pérennité de données chiffrées : divulgation de la clé de déchiffrement, abandon de l'algorithme cryptographique utilisé pour chiffrer les documents, changement de taille de clé supportée par le logiciel (l'ancienne devenant trop courte par rapport aux attaques possibles), bug dans le logiciel (pouvant rendre un déchiffrement impossible), et plus simplement disparition de la maintenance du logiciel de chiffrement utilisé.

Dans l'état actuel, une solution raisonnable est d'utiliser ces outils de chiffrement et d'effectuer régulièrement un archivage en clair de ses données. Cet archivage pourra être stocké dans un coffre-fort personnel si un besoin de confidentialité élevée est désiré.

Jean-Luc.Archimbaud@urec.cnrs.fr

Perspectives sur la recherche en cryptologie

Jacques Stern, Directeur du Laboratoire d'informatique de l'École normale supérieure (LIENS, UMR 8548),
Phong Nguyen et David Pointcheval, chargés de recherche au LIENS.

L'ubiquité de la cryptologie

Dans la société de l'information en émergence, 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 cryptographiques. Les algorithmes cryptographiques nous assurent que personne ne peut téléphoner à nos frais, intercepter notre numéro de carte de paiement sur la Toile, accéder aux données confidentielles de notre carte Vitale, etc. Bien sûr, les failles de sécurité n'ont souvent aucun rapport avec la cryptographie, ou éventuellement avec sa mise en œuvre (mauvais choix d'algorithmes ou de paramètres, implantations erronées). Cela étant, sans le recours à des mécanismes cryptographiques implantés de façon correcte, il est impossible d'éliminer les fraudes les plus sérieuses et les atteintes les plus graves à la confidentialité.

Qu'est-ce que la cryptologie ?

La *cryptologie* est la science des messages secrets. Longtemps restreinte aux usages diplomatiques et militaires, elle est maintenant une discipline scientifique à part entière, dont les applications sont si vastes aujourd'hui qu'il est difficile de définir a priori ce qui relève ou non de la cryptologie. Initialement, la cryptologie 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. Elle recouvre aujourd'hui l'ensemble des procédés informatiques devant résister à des adversaires, aussi redoutables et aussi mal intentionnés soient-ils, qui ne respectent pas les « règles du jeu ».

■ Un service d'intégrité garantit que le contenu d'une communication ou d'un fichier n'ont pas été modifié de façon malveillante.

■ Un service d'authenticité garantit l'identité d'une entité donnée ou l'ori-

gine 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, on parle de « non-répudiation ». Ce service de non-répudiation est réalisé par une signature numérique, qui a une valeur juridique depuis la loi du 20 mars 2000.

■ Un service de confidentialité garantit que le contenu d'une communication ou d'un fichier ne sont pas accessibles aux tiers. Des services de confidentialité sont offerts dans de nombreux contextes, notamment en téléphonie mobile, en télévision à péage et bien évidemment dans les navigateurs, par l'intermédiaire du protocole SSL/TLS.

La cryptologie se partage en deux sous-disciplines, également importantes : la *cryptographie*, dont l'objet est de proposer des méthodes pour assurer les services définis plus haut, et la *cryptanalyse*, qui étudie la sécurité apportée par les mécanismes proposés.

Pendant longtemps, les services d'intégrité, d'authenticité et de confidentialité ont été assurés par des algorithmes de chiffrement symétriques. Un tel algorithme utilise une *clé de chiffrement*, commune à l'émetteur et au destinataire d'un message. Il transforme un message clair en message chiffré ou cryptogramme. Un autre algorithme, appelé algorithme de déchiffrement, utilise la même clé pour restaurer le clair à partir du chiffré. Si l'on souhaite seulement garantir un service d'authenticité, la réversibilité n'est pas nécessaire et un seul algorithme suffit : le cryptogramme est joint au message et le récepteur peut simplement vérifier le calcul à l'aide de la clé. Cependant, la non-répudiation n'est pas assurée puisque tout détenteur de la clé – il y en a au moins deux – peut calculer ou vérifier le cryptogramme. La sécurité de l'algorithme est nominalement mesurée par la taille des clés supposées données sous forme d'une suite de bits (0 ou 1). La difficulté est de garantir qu'on ne peut faire mieux que de parcourir par recherche exhaustive l'espace des clés, soit pour des clés de n bits de l'ordre de 2^n exécutions. En 1976, Whitfield Diffie et Martin Hellman firent une découverte essentielle en

observant que la clé de chiffrement pouvait parfaitement être différente de la clé de déchiffrement, pour autant que la seconde ne se déduise pas facilement de la première, laquelle n'a pas à être gardée secrète : on parle de *clé publique*. Ce principe a été mis en œuvre dès 1978 dans l'algorithme RSA inventé par Rivest, Shamir et 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, un cryptogramme RSA (on dit plutôt une signature RSA), est vérifiable avec la seule clé publique, ce qui garantit la non-répudiation.

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. Sans pouvoir revenir sur tous ces travaux, nous voudrions ici évoquer trois axes de recherche prometteurs apparus dans les dernières années. Les thèmes choisis concernent des méthodes ou des protocoles concrets et opérationnels, étudiés notamment au sein de notre laboratoire. La description de recherches menées par d'autres spécialistes nécessiterait un autre article, qui pourrait notamment rendre compte des progrès de la cryptographie quantique et des travaux sur les calculateurs quantiques : ces machines, si elles voyaient le jour, pourraient factoriser les entiers de la cryptographie RSA. Mais on n'en est pas là !

Les fonctions de hachage

Une fonction de hachage est une fonction calculant efficacement un condensé de taille fixe à partir d'un message de longueur quelconque. Par définition, une telle fonction ne peut [..... suite page 6](#) ➔

— suite de la page 5 —

être injective: elle présente même une infinité de collisions, c'est-à-dire des couples de messages distincts mais dont le condensé est identique. D'un point de vue cryptographique, on souhaite cependant qu'il soit impossible de calculer en pratique de telles collisions. Cette propriété empêche ainsi la substitution d'un message à un autre, si le condensé est conservé séparément, ce qui permet d'assurer un service d'intégrité.

Le célèbre «paradoxe des anniversaires» montre qu'une fonction de hachage cryptographique doit renvoyer des condensés d'au moins $2n$ bits si l'on veut un niveau de sécurité de l'ordre de 2^n exécutions de la fonction. Dans les années quatre-vingt-dix, plusieurs fonctions de hachage ont été conçues et normalisées, MD5 (128 bits) et SHA1 (160 bits) notamment. Ces fonctions sont largement utilisées, notamment dans la génération des signatures RSA. Depuis une dizaine d'années, des travaux de cryptanalyse menés par divers chercheurs tendaient à indiquer des faiblesses potentielles de MD5 et SHA1. De fait, en 2005, une chercheuse chinoise Xiaoyun Wang et ses collaborateurs ont pu montrer que la sécurité de MD5 et celle de SHA1 étaient notablement plus faibles qu'attendu. Pour SHA1, le niveau de sécurité ne dépasse pas 2^{63} au lieu de 2^{80} . Même si la marge qui demeure est pour l'instant suffisante pour les applications, il est urgent que la communauté scientifique propose une nouvelle méthodologie pour concevoir des fonctions de hachage sûres et efficaces.

La sécurité prouvée

Le plus grand progrès qu'ait connu la cryptographie asymétrique depuis son invention est la méthodologie de la *sécurité prouvée*, 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 ainsi 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 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

En pratique, l'un des principaux problèmes de la cryptographie asymétrique est la gestion des clés 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 clés publiques d'être directement reliées à l'identité des utilisateurs: toute chaîne de caractères, par exemple une adresse électronique, est une clé publique potentielle.

Cela est rendu possible par l'intermédiaire d'une autorité en laquelle tous les utilisateurs ont confiance: l'autorité choisit des paramètres publics et à chaque fois qu'un utilisateur souhaite enregistrer une clé publique (de valeur arbitraire) l'utilisateur l'envoie à l'autorité, qui lui retourne la clé secrète correspondante. La cryptographie à base d'identité est en plein essor mais elle n'est pas sans inconvénient. En effet, elle a dû faire appel à des théories mathématiques complexes

dont l'aspect algorithmique n'a pas encore fait l'objet de recherches approfondies, comme le couplage de Weil sur les courbes elliptiques. Par ailleurs, l'auto-rité a alors nécessairement connaissance de toutes les clés secrètes, ce qui selon le contexte peut être souhaitable ou au contraire inacceptable.

Jacques.Stern@ens.fr
Phong.Nguyen@ens.fr
David.Pointcheval@ens.fr

■ Cryptologie: un important potentiel de recherche publique

Au CNRS (et en partenariat avec d'autres organismes: Ecole Normale Supérieure, Ecole Polytechnique, INRIA, Universités...), la cryptologie mobilise une vingtaine de laboratoires associés et plus d'une centaine de chercheurs, sur les aspects mathématiques et informatiques (méthodes de chiffrement, protocoles cryptographiques...) ainsi que sur les propriétés de la physique quantique pour sécuriser les informations.

Au plan gouvernemental, les recherches sont principalement conduites par le Centre Electronique de l'Armement (DGA/CELAR) et la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI). L'expertise gouvernementale s'appuie également sur les services spécialisés de la DGSE et du ministère de l'Intérieur (Centre Technique d'Assistance).

Pour en savoir plus: consulter la page consacrée au potentiel de recherche en cryptologie <http://www.sg.cnrs.fr/FSD/secure-systemes/revue.htm>
Contact: Robert Plana
(robert.plana@cnrs-dir.fr)

SÉCURITÉ INFORMATIQUE

numéro 55 décembre 2005
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités: tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité: 4 numéros par an.
Lectorat: toutes les formations CNRS.

Responsable de la publication:

JOSEPH ILLAND
Fonctionnaire de Sécurité de Défense
Centre national de la recherche scientifique
3, rue Michel-Ange, 75794 Paris XVI
Tél. 01 44 96 41 88
Courriel: Joseph.Illand@cnrs-dir.fr
<http://www.sg.cnrs.fr/fsd>

Rédacteur en chef de ce numéro:
JOSEPH ILLAND, CNRS/FSD

ISSN 1257-8819
Commission paritaire n° 1010 B 07548
La reproduction totale ou partielle des articles est autorisée sous réserve de mention d'origine