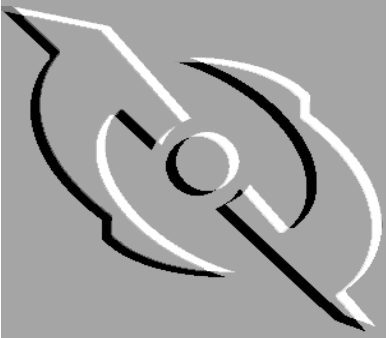

Introduction à la cryptographie

DROITS D'AUTEUR

Network Associates International BV. +31(20)5866100
Gatwickstraat 25
NL-1043 GL Amsterdam
http://www.nai.com

info@nai.com

Le signe * est parfois utilisé à la place de ® pour les marques déposées, afin de les protéger.

GARANTIE LIMITEE

Garantie limitée. Network Associates garantit, pour une période de (60) soixante jours à partir de la date d'achat d'origine, les supports (par exemple, disquettes) contenant le logiciel contre tout défaut de matériau et de fabrication.

Recours du client. La responsabilité de Network Associates et de ses fournisseurs et le recours exclusif du client seront limités, au choix de Network Associates, (i) au remboursement du prix d'achat de la licence, le cas échéant, ou (ii) au remplacement des supports défectueux contenant le logiciel avec une copie sur les supports non défectueux. Les supports défectueux doivent être renvoyés à Network Associates aux frais du client avec une copie du reçu. Cette garantie limitée n'est plus valable si le défaut a été provoqué par un accident, une utilisation abusive ou une mauvaise utilisation. Tout support de remplacement sera soumis à la période de garantie d'origine. Ce recours est limité aux Etats-Unis, car Network Associates est sujet à des restrictions régies par les lois et les décrets relatifs au contrôle des exportations aux Etats-Unis.

Limites de responsabilité. Dans les limites permises par la loi, à l'exception de la garantie limitée du présent document, LE LOGICIEL EST FOURNI « TEL QUEL » SANS GARANTIE, EXPRESSE OU IMPLICITE. SANS LIMITATION DES DISPOSITIONS SUSMENTIONNEES, LE CLIENT EST TENU RESPONSABLE DE LA SELECTION DU LOGICIEL POUR OBTENIR DES RESULTATS ATTENDUS ET POUR L'INSTALLATION, L'UTILISATION ET LES RESULTATS OBTENUS GRACE AU LOGICIEL. SANS LIMITATION DES DISPOSITIONS SUSMENTIONNEES, NETWORK ASSOCIATES N'OFFRE AUCUNE GARANTIE INDIQUANT QUE L'EXECUTION DU LOGICIEL SERA EXEMPTE D'ERREURS OU D'AUTRES DEFAUTS ET NE SERA PAS INTERROMPUE, OU QUE LE LOGICIEL REPONDE A DES BESOINS SPECIFIQUES. DANS LES LIMITES PERMISES PAR LA LOI, NETWORK ASSOCIATES DECLINE TOUTE RESPONSABILITE, EXPRESSE OU IMPLICITE, COMPRENANT MAIS NON LIMITEE AUX GARANTIES IMPLICITES DE VENTE, ADAPTATION A UN USAGE PARTICULIER ET NON RESPECT CONFORMEMENT AU LOGICIEL ET A SA DOCUMENTATION. CERTAINS ETATS ET JURIDICTIONS N'AUTORISENT PAS LA LIMITATION DES GARANTIES IMPLICITES. DANS DE TELS CAS, LA LIMITATION CI-DESSUS PEUT ETRE LIMITEE DANS SON APPLICATION. Les spécifications mentionnées sont applicables dans les limites permises par la loi.

Table des matières

Préface

La cryptographie est un sujet de roman d'espionnage et de bande dessinée d'action. Rares sont ceux n'ayant jamais vu un film ou un téléfilm mettant en scène un homme impossible à décrire, vêtu d'un costume et tenant une mallette accrochée à son poignet par des menottes. Le mot « espionnage » évoque James Bond, des courses poursuites en voiture et des balles sifflant aux oreilles.

Vous, vous êtes assis à votre bureau et vous devez remplir la tâche plutôt banale d'envoyer un document commercial à un collègue de telle sorte que personne d'autre ne puisse le lire. Vous devez simplement vous assurer que votre collègue est l'unique et véritable destinataire de l'e-mail et lui garantir que vous en êtes bien l'expéditeur. La sécurité nationale n'est pas en jeu, mais si un concurrent de votre entreprise s'emparait de ce document, il pourrait beaucoup vous en coûter. Comment pouvez-vous procéder ?

Vous pouvez recourir à la cryptographie. Peut-être aurez-vous le sentiment que l'aspect dramatique des phrases codées chuchotées dans de sombres couloirs fait défaut, mais le résultat est le même : les informations sont révélées uniquement aux personnes souhaitées.

A qui s'adresse ce guide ?

Ce guide est destiné à toute personne souhaitant connaître les bases de la cryptographie. Il fournit des explications sur la terminologie et la technologie que vous rencontrerez lors de l'utilisation des produits PGP. Il est utile de le lire avant de commencer à utiliser la cryptographie.

Comment utiliser ce guide ?

Ce guide décrit comment utiliser PGP afin de gérer en toute sécurité le stockage des données et des messages de votre entreprise.

Le Chapitre 1, « Notions élémentaires de cryptographie » donne un aperçu d'ensemble de la terminologie et des concepts relatifs aux produits PGP.

Le Chapitre 2, « Phil Zimmermann à propos de PGP », rédigé par le créateur de PGP, traite de la sécurité, de la confidentialité et des vulnérabilités inhérentes à tout système, même à PGP.

Pour plus d'informations

Pour plus d'informations sur le support technique et pour obtenir des réponses à d'éventuelles autres questions relatives au produit, reportez-vous au fichier What's New.

Lectures annexes

Les documents suivants peuvent vous être utiles afin de mieux comprendre la cryptographie :

Livres techniques et généralistes pour débutants

- « *Cryptography for the Internet* » de Philip R. Zimmermann. Scientific American, octobre 1998. Cet article, écrit par le créateur de PGP, est un cours sur différents protocoles et algorithmes de cryptographie, dont beaucoup sont utilisés par PGP.
- « *Privacy on the Line* » de Whitfield Diffie et Susan Eva Landau. MIT Press ; ISBN : 0262041677. Ce livre traite de l'histoire et de la politique gravitant autour de la cryptographie et de la sécurité des communications. Il constitue une excellente lecture, même pour les débutants et le personnel non technique, et contient des informations que même de nombreux experts ignorent.
- « *The Codebreakers* » de David Kahn. Scribner ; ISBN : 0684831309. Ce livre relate l'histoire des codes et des casseurs de codes depuis le temps des Egyptiens jusqu'à la fin de la seconde guerre mondiale. Kahn l'a écrit dans les années soixante, puis en a publié une version révisée en 1996. Ce livre ne vous apprendra rien sur le mode de fonctionnement de la cryptographie, mais il a inspiré toute la nouvelle génération de cryptographes.
- *« Network Security : Private Communication in a Public World »* de Charlie Kaufman, Radia Perlman et Mike Spencer Prentice Hall ; ISBN : 0-13-061466-1. Cet ouvrage fournit une description détaillée des systèmes et des protocoles de sécurité de réseau, notamment des explications sur leur bon ou mauvais fonctionnement. Publié en 1995, il traite peu des dernières avancées technologiques, mais reste un livre intéressant. Il contient également une des descriptions les plus claires sur le fonctionnement du DES parmi tous les livres écrits sur le sujet.

Livres intermédiaires

- « *Applied Cryptography : Protocols, Algorithms, and Source Code in C* » de Bruce Schneier, John Wiley & Sons ; ISBN : 0-471-12845-7. Il s'agit d'un bon livre technique pour se familiariser avec le fonctionnement d'une grande partie de la cryptographie. Si vous souhaitez devenir un expert, c'est le livre qu'il vous faut pour commencer.

- « *Handbook of Applied Cryptography* » d'Alfred J. Menezes, Paul C. van Oorschot et Scott Vanstone. CRC Press ; ISBN : 0-8493-8523-7. Voici le livre technique qu'il vous faut lire après le livre de Schneier. Le niveau mathématique de ce livre est très élevé, mais celui-ci reste cependant utilisable par ceux qui ne maîtrisent pas bien cette matière.

- « *Internet Cryptography* » de Richard E. Smith. Addison-Wesley Pub Co ; ISBN : 0201924803. Ce livre décrit le mode de fonctionnement de nombreux protocoles de sécurité Internet. Il décrit notamment comment des systèmes bien conçus finissent cependant par présenter des défaillances suite à une utilisation négligente. Cet ouvrage contient peu de notions mathématiques et beaucoup d'informations pratiques.

- « *Firewalls and Internet Security : Repelling the Wily Hacker* » de William R. Cheswick et Steven M. Bellovin. Addison-Wesley Pub Co ; ISBN : 0201633574. Ce livre a été écrit par deux éminents chercheurs de chez AT&T Bell Labs et traite de leurs expériences dans le maintien et la restructuration des connexions Internet de AT&T. Très accessible.

Livres très techniques

- « *A Course in Number Theory and Cryptography* » de Neal Koblitz. Springer-Verlag ; ISBN : 0-387-94293-9. Il s'agit d'un excellent manuel universitaire de mathématiques sur la théorie des nombres et la cryptographie.

- « *Differential Cryptanalysis of the Data Encryption Standar*d » de Eli Biham et Adi Shamir. Springer-Verlag ; ISBN : 0-387-97930-1. Ce livre décrit la technique de cryptanalyse différentielle telle qu'elle est appliquée au DES. C'est un excellent ouvrage pour apprendre cette technique.

Notions élémentaires de cryptographie 1

Lorsque Jules César envoyait des messages à ses généraux, il ne faisait pas confiance à ses messagers. Il remplaçait donc tous les A contenus dans ses messages par des D, les B par des E, et ainsi de suite pour tout l'alphabet. Seule la personne connaissant la règle du « décalage par trois » pouvait déchiffrer ses messages.

Et voilà comment tout a commencé.

Cryptage et décryptage

Les données lisibles et compréhensibles sans intervention spécifique sont considérées comme du *texte en clair*. La méthode permettant de dissimuler du texte en clair en masquant son contenu est appelée le *cryptage*. Le cryptage consiste à transformer un texte normal en charabia inintelligible appelé *texte chiffré*. Cette opération permet de s'assurer que seules les personnes auxquelles les informations sont destinées pourront y accéder. Le processus inverse de transformation du texte chiffré vers le texte d'origine est appelé le *décryptage*.

La Figure 1-1 illustre ce processus.

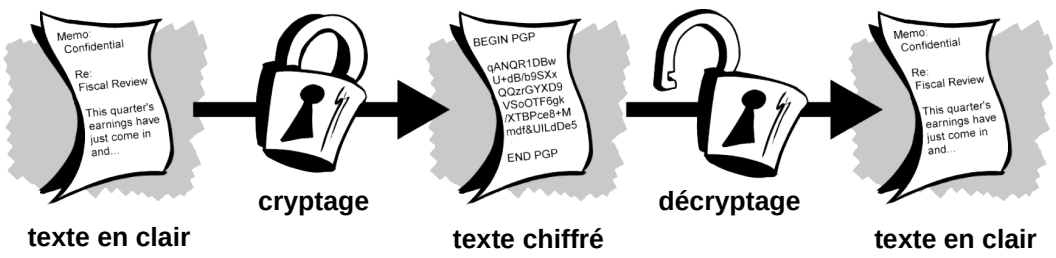

Figure 1-1. Cryptage et décryptage

Définition de la cryptographie

La *cryptograpie* est la science qui utilise les mathématiques pour le cryptage et le décryptage de données.

Elle vous permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse les lire.

Alors que la cryptographie consiste à sécuriser les données, la *cryptanalyse* est l'étude des informations cryptées, afin d'en découvrir le secret. La cryptanalyse classique implique une combinaison intéressante de raisonnement analytique, d'application d'outils mathématiques, de recherche de modèle, de patience, de détermination et de chance. Ces cryptanalystes sont également appelés des *pirates*.

La *cryptologie* englobe la cryptographie et la cryptanalyse.

Cryptographie invulnérable

« Il existe deux types de cryptographie dans le monde : la cryptographie qui protège vos documents de la curiosité de votre petite sœur et celle qui empêche les gouvernements les plus puissants de lire vos fichiers. Cet ouvrage s'adresse au dernier cas. »

—Bruce Schneier, Applied Cryptography : Protocols, Algorithms, and Source Code in C.

PGP traite également de ce dernier type de cryptographie.

La cryptographie peut être *invulnérable* ou *vulnérable*, comme décrit précédemment. Cette vulnérabilité se mesure en termes de temps et de ressources nécessaires pour récupérer le texte en clair. Une *cryptographie invulnérable* pourrait être définie comme un texte crypté particulièrement difficile à déchiffrer sans l'aide d'un outil de décodage approprié. Mais, alors, comment déterminer cette difficulté ? Etant donné la puissance informatique et le temps machine actuellement disponibles, il devrait être impossible de déchiffrer le résultat d'une telle cryptographie avant la fin du monde (même avec un milliard d'ordinateurs effectuant un milliard de vérifications à la seconde).

On pourrait donc penser qu'une cryptographie évoluée résisterait même aux assauts d'un cryptanalyste particulièrement acharné. Qui peut vraiment l'affirmer ? Personne n'a encore prouvé que le meilleur niveau de cryptage pouvant être obtenu de nos jours tiendra la route avec la puissance informatique de demain. Néanmoins, nous pouvons vous assurer que PGP est actuellement la solution la plus invulnérable à ce jour. La vigilance et la prudence constituent toutefois une meilleure protection que les prétentions d'inviolabilité.

Mécanismes de la cryptographie

Un *algorithme de cryptographie* ou un *chiffrement* est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est associé à une *clé* (un mot, un nombre ou une phrase), afin de crypter le texte en clair. Avec des clés différentes, le résultat du cryptage variera également. La sécurité des données cryptées repose entièrement sur deux éléments : l'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clé.

Un *système de cryptographie* est constitué d'un algorithme de cryptographie, ainsi que de toutes les clés et tous les protocoles nécessaires à son fonctionnement. PGP est un système de cryptographie.

Cryptographie conventionnelle

En cryptographie conventionnelle, également appelée cryptage de *clé secrète* ou de *clé symétrique*, une seule clé suffit pour le cryptage et le décryptage. La norme de cryptage de données (DES) est un exemple de système de cryptographie conventionnelle largement utilisé par le gouvernement fédéral des Etats-Unis. La Figure 1-2 est une illustration du processus de cryptage conventionnel.

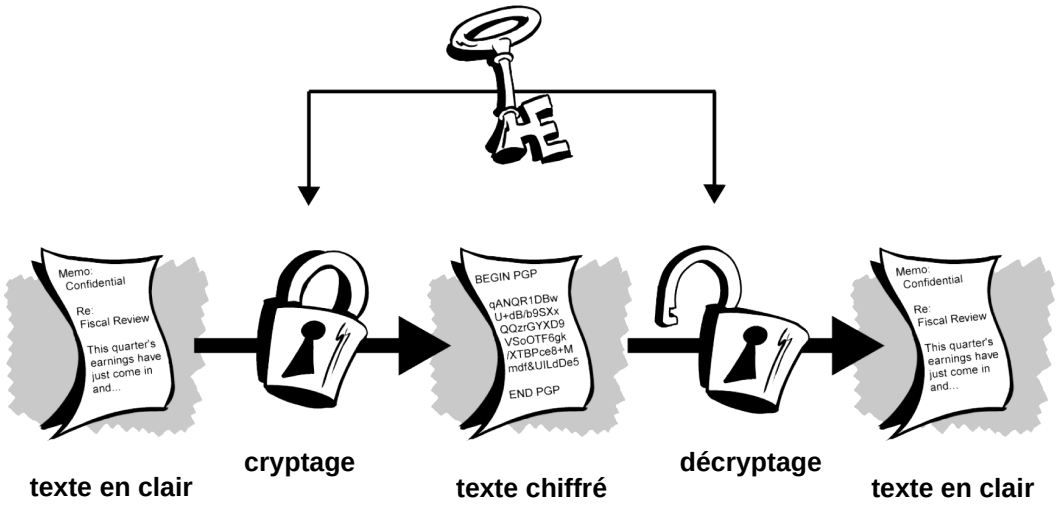

Figure 1-2. Cryptage conventionnel

Chiffrement de César

Le chiffrement de substitution est un exemple extrêmement simple de cryptographie conventionnelle. Il substitue une information par une autre. Cette opération s'effectue généralement en décalant les lettres de l'alphabet. Le code secret de Jules César est à la base de la cryptographie conventionnelle. Dans ce cas, l'algorithme constitue à décaler les lettres de l'alphabet et la clé correspond au nombre de caractères de décalage.

Par exemple, si vous codez le mot « SECRET » à l'aide de la valeur 3 de la clé de César, l'alphabet est décalé de manière à commencer à la lettre D.

Ainsi, l'alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

si vous décalez le début de 3 lettres, vous obtenez

DEFGHIJKLMNOPQRSTUVWXYZABC

où D = A, E = B, F = C, etc.

Avec ce procédé, le texte en clair « SECRET » est crypté en « VHFUHW ». Pour autoriser un autre utilisateur à lire le texte chiffré, indiquez-lui que la valeur de la clé est égale à 3.

Evidemment, ceci est considéré comme une cryptographie extrêmement vulnérable de par les standards actuels. Mais, cette méthode convenait à César et illustre le mode de fonctionnement de la cryptographie conventionnelle.

Gestion des clés et cryptage conventionnel

Le cryptage conventionnel comporte des avantages. Il est très rapide. Mais, il s'avère particulièrement utile pour les données véhiculées par des *moyens de transmission* sécurisés. Toutefois, il peut entraîner des coûts importants en raison de la difficulté à garantir la confidentialité d'une clé de cryptage lors de la distribution.

Souvenez-vous d'un personnage de votre film d'espionnage préféré : la personne avec un porte-documents menotté à son poignet. Mais que contient donc ce porte-documents ? Sûrement pas le code de lancement d'un missile, la formule d'une biotoxine ou un plan d'invasion, mais la *clé* permettant de décrypter ces données secrètes.

Un expéditeur et un destinataire souhaitant communiquer de manière sécurisée à l'aide du cryptage conventionnel doivent convenir d'une clé et ne pas la divulguer. S'ils se trouvent à des emplacements géographiques différents, ils doivent faire confiance à un coursier, au téléphone de Batman ou à tout autre moyen de communication sécurisé pour éviter la divulgation de la clé secrète lors de la transmission. Toute personne interceptant la clé lors d'un transfert peut ensuite lire, modifier et falsifier toutes les informations cryptées ou authentifiées avec cette clé. De la norme de cryptage de données DES au code secret de Jules César, la *distribution des clés* reste le problème majeur du cryptage conventionnel. Autrement dit, comment faire parvenir la clé à son destinataire sans qu'aucune personne ne l'intercepte ?

Cryptographie de clé publique

Les problèmes de distribution des clés sont résolus par la *cryptographie de clé publique*. Ce concept a été introduit par Whitfield Diffie et Martin Hellman en 1975. (Il est maintenant prouvé que les services secrets britanniques avaient fait cette même découverte plusieurs années avant Diffie et Hellman et avaient protégé ce secret militaire (sans en faire aucune utilisation).[1]

La cryptographie de clé publique est un procédé asymétrique utilisant une *paire* de clés pour le cryptage : une *clé publique* qui crypte des données et une *clé privée* ou *secrète* correspondante pour le décryptage. Vous pouvez ainsi publier votre clé publique tout en conservant votre clé privée secrète. Tout utilisateur possédant une copie de votre clé publique peut ensuite crypter des informations que vous êtes le seul à pourvoir lire. Même les personnes que vous ne connaissez pas personnellement peuvent utiliser votre clé publique.

D'un point de vue informatique, il est impossible de deviner la clé privée à partir de la clé publique. Tout utilisateur possédant une clé publique peut crypter des informations, mais est dans l'impossibilité de les décrypter. Seule la personne disposant de la clé privée correspondante peut les décrypter.

1. J H Ellis, The Possibility of Secure Non-Secret Digital Encryption, Rapport du CESG, janvier 1970. [Le CESG est l'institution nationale britannique responsable de l'utilisation officielle de la cryptographie.]

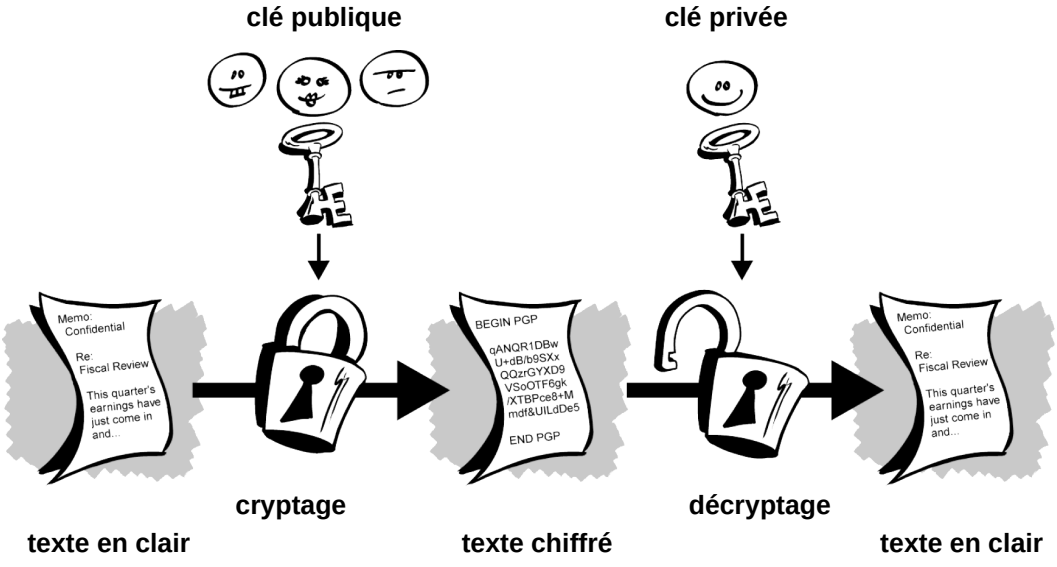

Figure 1-3. Cryptage de clé publique

La cryptographie de clé publique présente un avantage majeur : en effet, elle permet d'échanger des messages de manière sécurisée sans aucun dispositif de sécurité. L'expéditeur et le destinataire n'ont plus besoin de partager des clés secrètes via une voie de transmission sécurisée. Les communications impliquent uniquement l'utilisation de clés publiques et plus aucune clé privée n'est transmise ou partagée. Elgamal (d'après le nom de son inventeur, Taher Elgamal), RSA (d'après le nom de ses inventeurs, Ron Rivest, Adi Shamir et Leonard Adleman), Diffie-Hellman (également d'après le nom de ses inventeurs) et DSA, l'algorithme de signature numérique (élaboré par David Kravitz), sont des exemples de systèmes de cryptographie de clé publique.

La cryptographie conventionnelle étant auparavant la seule méthode pour transmettre des informations secrètes, les coûts de transmission et de distribution sécurisées des clés ont relégué son utilisation aux institutions disposant de moyens suffisants, telles que des gouvernements et des banques.
Le cryptage de clé publique représente une révolution technologique qui offre à tout citoyen la possibilité d'utiliser une cryptographie invulnérable. Souvenez-vous du messager avec un porte-documents menotté à son poignet.
Le cryptage de clé publique l'a mis au chômage (probablement à son grand soulagement).

Fonctionnement de PGP

PGP est une combinaison des meilleures fonctionnalités de la cryptographie de clé publique et de la cryptographie conventionnelle. PGP est un *système de cryptographie hybride*.

Lorsqu'un utilisateur crypte du texte en clair avec PGP, ces données sont d'abord compressées. Cette compression des données permet de réduire le temps de transmission par modem, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique. La plupart des cryptanalystes exploitent les modèles trouvés dans le texte en clair pour casser le chiffrement. La compression réduit ces modèles dans le texte en clair, améliorant par conséquent considérablement la résistance à la cryptanalyse. Toutefois, la compression est impossible sur les fichiers de taille insuffisante ou supportant mal ce processus.

PGP crée ensuite une *clé de session* qui est une clé secrète à usage unique. Cette clé correspond à un nombre aléatoire, généré par les déplacements aléatoires de votre souris et les séquences de frappes de touches. Pour crypter le texte en clair, cette clé de session utilise un algorithme de cryptage conventionnel rapide et sécurisé. Une fois les données codées, la clé de session est cryptée vers la clé publique du destinataire. Cette clé de session cryptée par clé publique est transmise avec le texte chiffré au destinataire.

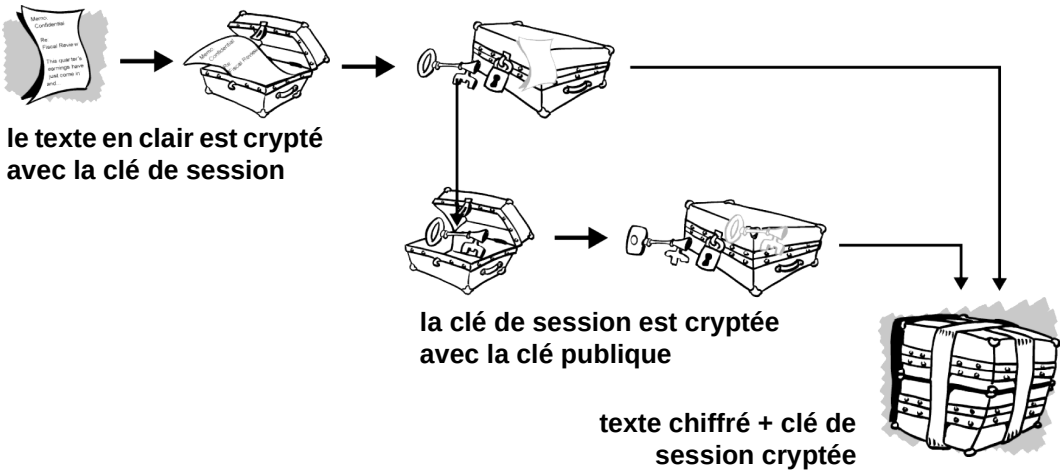

Figure 1-4. Fonctionnement du cryptage PGP

Le processus de décryptage est inverse. La copie de PGP du destinataire utilise sa clé privée pour récupérer la clé de session temporaire qui permettra ensuite de décrypter le texte crypté de manière conventionnelle.

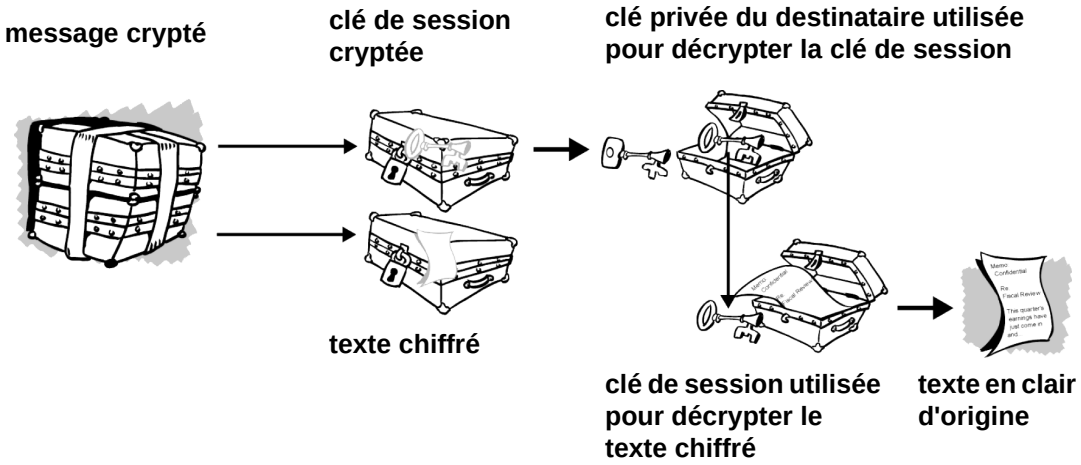

Figure 1-5. Fonctionnement du décryptage PGP

Ces deux méthodes de cryptage associent la facilité d'utilisation du cryptage de clé publique à la vitesse du cryptage conventionnel. Le cryptage conventionnel est environ 1 000 fois plus rapide que le cryptage de clé publique. De plus, le cryptage de clé publique résout non seulement le problème de la distribution des clés, mais également de la transmission des données. Utilisées conjointement, ces deux méthodes améliorent la performance et la distribution des clés, sans pour autant compromettre la sécurité.

Clés

Une clé est une valeur utilisée dans un algorithme de cryptographie, afin de générer un texte chiffré. Les clés sont en réalité des nombres extrêmement importants. La taille d'une clé se mesure en bits et le nombre correspondant à une clé de 1 024 bits est gigantesque. Dans la cryptographie de clé publique, plus la clé est grande, plus la sécurité du texte chiffré est élevée.

Cependant, la taille de la clé publique et de la clé secrète de cryptographie conventionnelle sont complètement indépendantes. Une clé conventionnelle de 80 bits est aussi puissante qu'une clé publique de 1 024 bits. De même, une clé conventionnelle de 128 bits équivaut à une clé publique de 3 000 bits. Encore une fois, plus la clé est grande, plus elle est sécurisée, mais les algorithmes utilisés pour chaque type de cryptographie sont très différents. Autant essayer de comparer une pomme avec une orange.

Même si les clés publiques et privées sont liées par une relation mathématique, il est très difficile de deviner la clé privée uniquement à partir de la clé publique. Cependant, la déduction de la clé privée est toujours possible en disposant de temps et de puissantes ressources informatiques. Ainsi, il est très important de sélectionner des clés de tailles correctes, suffisamment grandes pour être sécurisées, mais suffisamment petites pour être utilisées assez rapidement. De plus, vous devez tenir compte du profil des utilisateurs tentant de lire vos fichiers, connaître leur détermination, le temps dont ils disposent, ainsi que de leurs ressources.

Plus la clé est grande, plus sa durée de sécurisation est élevée. Si les informations que vous souhaitez crypter doivent rester confidentielles pendant plusieurs années, vous pouvez utiliser une clé correspondant à un nombre de bits extrêmement élevé. Qui sait combien de temps sera nécessaire pour deviner votre clé avec la technologie de demain ? Il fut un temps où une clé symétrique de 56 bits était considérée comme extrêmement sûre.

Les clés sont stockées sous forme cryptée. PGP conserve les clés sur votre disque dur, dans deux fichiers : l'un est destiné aux clés publiques, l'autre aux clés privées. Ces fichiers s'appellent des *trousseaux de clés*. Lors de l'utilisation de PGP, vous devez généralement ajouter les clés publiques de vos destinataires sur votre trousseau de clés publiques. Vos clés privées sont stockées sur votre trousseau de clés privées. En cas de perte de votre trousseau de clés privées, il vous sera impossible de décrypter les informations cryptées vers les clés de ce trousseau.

Signatures numériques

L'un des principaux avantages de la cryptographie de clé publique est qu'elle offre une méthode d'utilisation des *signatures numériques*. Celles-ci permettent au destinataire de vérifier leur authenticité, leur origine, mais également de s'assurer qu'elles sont intactes. Ainsi, les signatures numériques de clé publique garantissent l'*authentification* et l'*intégrité* des données. Elles fournissent également une fonctionnalité de *non répudiation*, afin d'éviter que l'expéditeur ne prétende qu'il n'a pas envoyé les informations. Ces fonctions jouent un rôle tout aussi important pour la cryptographie que la confidentialité, sinon plus.

Une signature numérique a la même utilité qu'une signature manuscrite. Cependant, une signature manuscrite peut être facilement imitée, alors qu'une signature numérique est pratiquement infalsifiable. De plus, elle atteste du contenu des informations, ainsi que de l'identification du signataire.

Certaines personnes privilégient l'utilisation des signatures par rapport au cryptage. Par exemple, qu'une personne sache que vous venez de déposer 5 000,00 FF sur votre compte vous importe peu. Cependant, vous voulez être certain d'avoir eu affaire à un caissier.

La Figure 1-6 illustre la méthode de création des signatures numériques. Plutôt que de crypter des informations avec la clé publique d'un autre utilisateur, cryptez-les avec votre clé privée. Si des informations peuvent être décryptées avec votre clé publique, c'est vous qui devez les avoir créées.

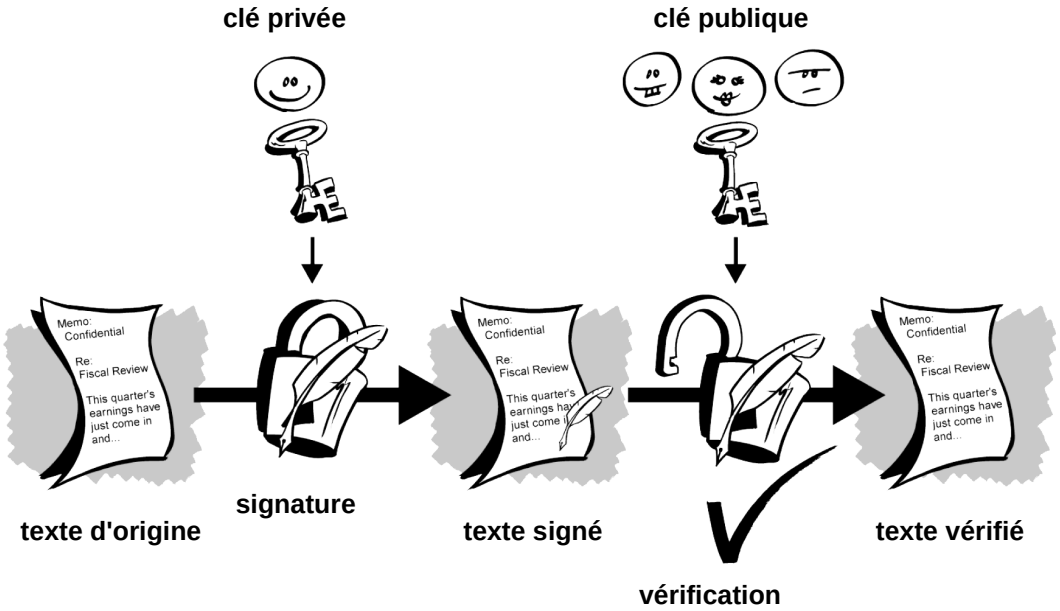

Figure 1-6. Signatures numériques simples

Fonctions de hachage

Le système décrit précédemment comporte certains problèmes. Il est lent et produit un volume important de données (au moins le double de la taille des informations d'origine). L'ajout d'une *fonction de hachage* à sens unique dans le processus permet d'améliorer le schéma ci-dessus. Cette fonction traite une entrée de longueur variable (dans ce cas, un message pouvant contenir indifféremment des milliers ou des millions de bits), afin d'obtenir en sortie un élément de longueur fixe, à savoir 160 bits. En cas de modification des données (même d'un seul bit), la fonction de hachage garantit la production d'une valeur de sortie complètement différente.

PGP applique au texte en clair signé par l'utilisateur une fonction de hachage évoluée, qui génère un élément de données à longueur définie, appelé *résumé de message*. En outre, toute modification apportée aux informations entraîne un résumé complètement différent.

PGP utilise ensuite le résumé et la clé privée pour créer la « signature ». PGP transmet en même temps la signature et le texte en clair. A réception du message, le destinataire utilise PGP pour traiter à nouveau le message informatiquement, vérifiant ainsi la signature. PGP peut crypter ou non le texte en clair. La signature du texte en clair est utile si certains utilisateurs ne souhaitent pas ou ne peuvent pas vérifier la signature.

Si une fonction de hachage sécurisée est utilisée, il est impossible de récupérer la signature d'un document pour la joindre à un autre document ou d'altérer un message signé. La moindre modification apportée à un document signé entraîne l'échec du processus de vérification de la signature numérique.

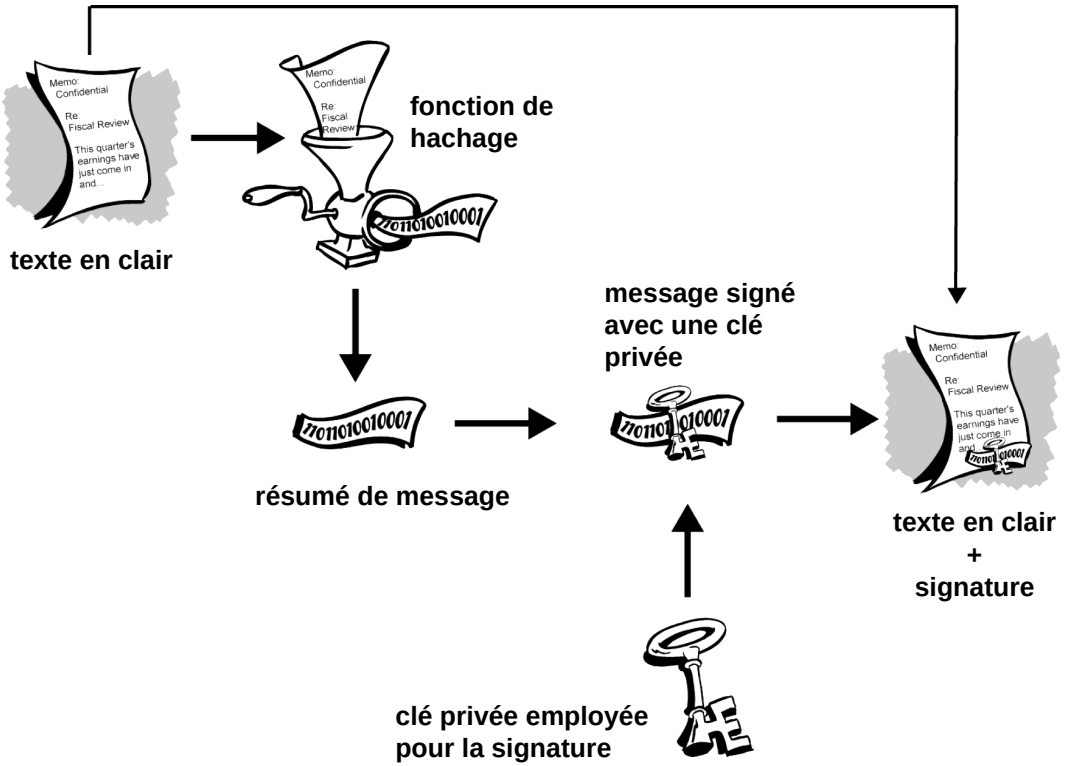

Figure 1-7. Signatures numériques sécurisées

Les signatures numériques jouent un rôle majeur dans l'authentification et la *validation* des clés d'autres utilisateurs PGP.

Certificats numériques

Lors de l'utilisation des systèmes de cryptographie de clé publique, les utilisateurs doivent constamment vérifier qu'ils cryptent vers la clé du bon utilisateur, ce qui constitue un problème. Dans un environnement où le libre échange de clés via des serveurs publics est sécurisé, toute attaque menée par une personne intermédiaire, encore appelée un *intercepteur*, représente une menace éventuelle. Dans ce type d'attaque, une personne place une fausse clé comportant le nom et l'ID utilisateur du destinataire. Les données cryptées (et interceptées) vers le détenteur réel de cette clé erronée sont dorénavant entre de mauvaises mains.

Dans un environnement de clé publique, il est essentiel de s'assurer que la clé publique vers laquelle vous cryptez les données est celle du destinataire concerné et non une contrefaçon. Vous pouvez crypter uniquement vers les clés qui vous ont été distribuées physiquement. Supposons maintenant que vous devez échanger des informations avec des personnes que vous ne connaissez pas, comment savoir que vous êtes en possession de la bonne clé ?

Les *certificats numériques* ou *certificats* simplifient la tâche qui consiste à déterminer si une clé publique appartient réellement à son détenteur supposé.

Un certificat correspond à une référence. Il peut s'agir par exemple de votre permis de conduire, de votre carte de sécurité sociale ou de votre certificat de naissance. Chacun de ces éléments contient des informations vous identifiant et déclarant qu'une autre personne a confirmé votre identité. Certains certificats, tels que votre passeport, représentent une confirmation de votre identité suffisamment importante pour ne pas les perdre, de crainte qu'une autre personne ne les utilise pour usurper votre identité.

Un certificat numérique contient des données similaires à celles d'un certificat physique. Il contient des informations associées à la clé publique d'une personne, aidant d'autres personnes à vérifier qu'une clé est authentique ou *valide*. Les certificats numériques permettent de contrecarrer les tentatives de substitution de la clé d'une personne par une autre.

Un certificat numérique se compose de trois éléments :

- Une clé publique.
- Des informations sur le certificat. (Informations sur l'« identité » de l'utilisateur, telles que son nom, son ID utilisateur, etc.)
- Une ou plusieurs signatures numériques.

La signature numérique d'un certificat permet de déclarer que ses informations ont été attestées par une autre personne ou entité. La signature numérique ne garantit pas totalement l'authenticité du certificat. Elle confirme uniquement que les informations d'identification signées correspondent ou *sont liées* à la clé publique.

Ainsi, un certificat équivaut en réalité à une clé publique comportant un ou deux types d'ID joints ainsi qu'une estampille agréée par d'autres personnes fiables.

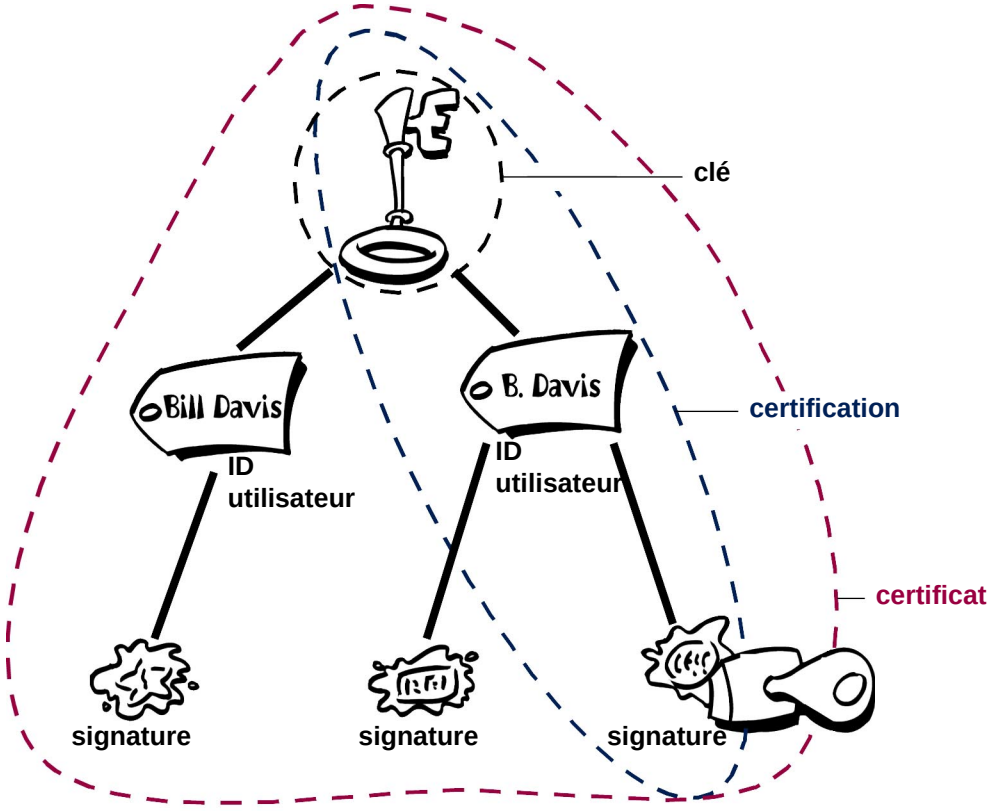

Figure 1-8. Schéma d'un certificat PGP

Distribution de certificats

Les certificats sont utilisés lors de l'échange de clés publiques avec un autre utilisateur. Pour un petit groupe de personnes souhaitant communiquer de manière sécurisée, il est facile d'échanger manuellement des disquettes ou des e-mails contenant la clé publique de chaque détenteur. Cette *distribution manuelle de clés publiques* s'avère limitée. Au-delà d'un certain point, il est nécessaire de mettre en place des systèmes pouvant fournir des mécanismes de sécurité, de stockage et d'échanges nécessaires pour que vos collègues ou d'autres personnes puissent communiquer. Ces systèmes peuvent se présenter sous la forme de référentiels de stockage uniquement, appelés *serveurs de certificats* ou sous la forme de systèmes structurés offrant des fonctions de gestion de clés, appelés *infrastructures de clé publique (PKI*).

Serveurs de certificats

Un *serveur de certificats*, également appelé *serveur de clés*, est une base de données permettant aux utilisateurs de soumettre et de récupérer des certificats numériques. Un serveur de certificats offre généralement des fonctions de gestion permettant à une entreprise de soutenir sa politique de sécurité (par exemple, autoriser uniquement le stockage des clés répondant à des exigences spécifiques).

Infrastructures de clé publique

Une PKI contient les fonctions de stockage de certificats d'un serveur de certificats, mais elle offre également des fonctions de gestion de certificats (émission, révocation, stockage, récupération et fiabilité des certificats). La principale fonction d'une PKI est de présenter l'*autorité de certification* ou la *CA*, à savoir une entité humaine (une personne, un groupe, un service, une entreprise ou une autre association) autorisée par une société à émettre des certificats à l'attention de ses utilisateurs informatiques. Une CA fonctionne comme un service de contrôle des passeports du gouvernement d'un pays. Elle crée des certificats et les signe de façon numérique à l'aide d'une clé privée de CA. Ainsi, la CA est l'élément central d'une PKI. A l'aide de la clé publique de la CA, quiconque souhaite vérifier l'authenticité d'un certificat doit vérifier la signature numérique de la CA émettrice et, par conséquent, l'intégrité du contenu du certificat (essentiellement, la clé publique et l'identité du détenteur du certificat).

Formats de certificats

Un certificat numérique est en réalité un ensemble d'informations permettant d'identifier une clé publique, signé par un tiers de confiance, afin de prouver son authenticité. Un certificat numérique peut se présenter sous différents *formats*.

PGP reconnaît deux formats de certificat :

- Certificats PGP
- Certificats X.509

Format de certificat PGP

Un certificat PGP comprend, entre autres, les informations suivantes :

- **Le numéro de version de PGP** : identifie la version de PGP utilisée pour créer la clé associée au certificat.
- **La clé publique du détenteur du certificat** : partie publique de votre paire de clés associée à l'algorithme de la clé, qu'il soit RSA, DH (Diffie-Hellman) ou DSA (Algorithme de signature numérique).
- **Les informations du détenteur du certificat** : il s'agit des informations portant sur l'« identité » de l'utilisateur, telles que son nom, son ID utilisateur, sa photographie, etc.
- **La signature numérique du détenteur du certificat** : également appelée *auto-signature*, il s'agit de la signature effectuée avec la clé privée correspondant à la clé publique associée au certificat.
- **La période de validité du certificat** : dates / heures de début et d'expiration du certificat. Indique la date d'expiration du certificat.
- **L'algorithme de cryptage symétrique préféré pour la clé** : indique l'algorithme de cryptage que le détenteur du certificat préfère appliquer au cryptage des informations. Les algorithmes pris en charge sont CAST, IDEA ou DES triple.

On peut comparer un certificat PGP à une clé publique comportant un ou plusieurs libellés (voir Figure 1-9). Dans ces « libellés » figurent des informations liées à l'identification du détenteur de la clé, ainsi que sa signature, confirmant l'association de la clé et de l'identification. Cette signature spécifique est appelée *auto-signature*- et figure dans chaque certificat PGP.

Le fait qu'un seul certificat puisse contenir plusieurs signatures est l'un des aspects uniques du format du certificat PGP. Plusieurs personnes peuvent signer la paire de clés / d'identification pour attester en toute certitude de l'appartenance de la clé publique au détenteur spécifié. Sur un serveur de certificats publics, vous pouvez remarquer que certains certificats, tels que celui du créateur de PGP, Phil Zimmermann, contiennent plusieurs signatures.

Certains certificats PGP sont composés d'une clé publique avec plusieurs libellés, chacun offrant un mode d'identification du détenteur de la clé différent (par exemple, le nom et le compte de messagerie d'entreprise du détenteur, l'alias et le compte de messagerie personnel du détenteur, sa photographie, et ce, dans un seul certificat). La liste des signatures de chacune de ces identités peut varier. Les signatures attestent de l'authenticité de l'appartenance de l'un des libellés à la clé publique et non de l'authenticité de tous les libellés sur la clé. Notez que « authentique » est fonction de l'opinion de l'utilisateur. Les signatures sont des opinions et différentes personnes vérifient à différents niveaux l'authenticité avant de signer une clé.

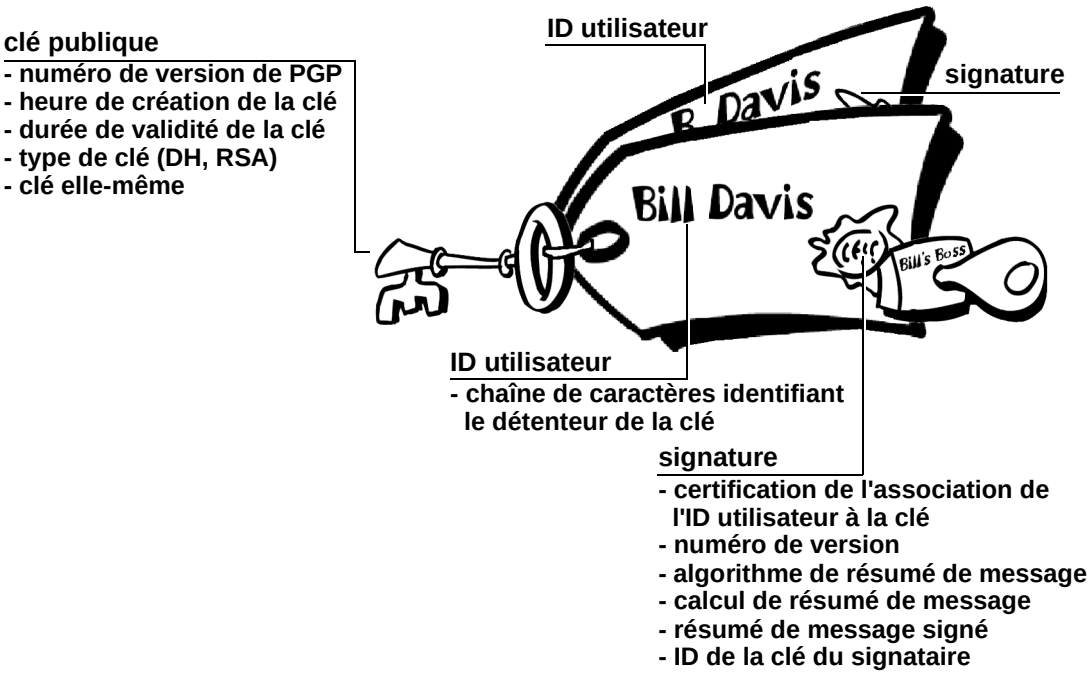

Figure 1-9. Un certificat PGP

Format de certificat X.509

Le format *X.509* est un autre format de certificat très utilisé. Tous les certificats X.509 sont conformes à la norme internationale UIT-T X.509. Ainsi, en théorie, les certificats X.509 créés pour une application peuvent être utilisés par toute autre application compatible X.509. Cependant, en pratique, différentes entreprises ont créé leurs propres extensions de certificats X.509, toutes n'étant pas compatibles.

Dans un certificat, une personne doit affirmer qu'une clé publique et le nom du détenteur de la clé sont associés. Quiconque peut valider les certificats PGP. Les certificats X.509 doivent toujours être validés par une autorité de certification ou une personne désignée par la CA. Gardez à l'esprit que les certificats PGP prennent également en charge une structure hiérarchique à l'aide d'une *CA* pour la validation des certificats.

Un certificat X.509 est un ensemble standard de champs contenant des informations relatives à un utilisateur ou un périphérique et à la clé publique correspondante. Le standard X.509 définit les informations à inclure dans le certificat et décrit leur mode de codage (le format des données). Tous les certificats X.509 contiennent les données suivantes :

- **Le numéro de version X.509** : identifie la version du standard X.509 s'appliquant à ce certificat, ce qui détermine les informations à spécifier. La version 3 est la plus courante.
- **La clé publique du détenteur du certificat** : clé publique du détenteur du certificat associée à un identifiant d'algorithme spécifiant le système de cryptographie auquel appartient la clé ainsi que tous les paramètres de clé correspondants.
- **Le numéro de série du certificat** : l'entité (application ou personne) ayant créé le certificat doit lui affecter un numéro de série unique permettant de le distinguer des autres certificats émis. Ces informations sont utilisées de différentes manières. Par exemple, lorsqu'un certificat est révoqué, son numéro de série est placé dans une *liste des révocations de certificats* ou *LRC*.
- **L'identifiant unique du détenteur du certificat** (ou *nom explicite* / *DN*). Ce nom doit être unique sur Internet. Un DN se compose de plusieurs sous-sections et peut avoir la structure suivante :

  NC = Robert Durand, UO = Service de sécurité réseau, O = Network Associates, Inc., C = France

  Ces éléments se réfèrent au nom, à l'unité organisationnelle, à l'organisme et au pays du sujet.

- **La période de validité du certificat** : dates / heures de début et d'expiration du certificat. Indique la date d'expiration du certificat.
- **Le nom unique de l'émetteur du certificat** : nom unique de l'entité ayant signé le certificat. Il s'agit généralement d'une CA. L'utilisation du certificat implique que vous faites confiance à l'entité ayant signé le certificat. Notez que dans certains cas, tels que pour les certificats CA de *haut* ou *bas niveau*, l'émetteur signe son propre certificat.
- **La signature numérique de l'émetteur** : signature effectuée avec la clé privée de l'entité ayant émis le certificat.
- **L'identifiant d'algorithme de signature** : identifie l'algorithme utilisé par la CA pour signer le certificat.

Plusieurs différences existent entre un certificat X.509 et un certificat PGP. Les plus importantes sont indiquées ci-dessous :

- Pour créer votre propre certificat PGP, vous devez demander l'émission d'un certificat X.509 auprès d'une autorité de certification et l'obtenir.
- Les certificats X.509 prennent en charge un seul nom pour le détenteur de la clé.
- Les certificats X.509 prennent en charge une seule signature numérique pour attester de la validité de la clé.

Pour obtenir un certificat X.509, demandez à une CA d'émettre un certificat à votre attention. Fournissez votre clé publique, preuve que vous possédez la clé privée correspondante, ainsi que des informations spécifiques vous concernant. Signez ensuite les informations numériquement, puis envoyez l'ensemble (la *demande* de certificat) à la CA. Cette dernière vérifie ensuite avec précaution que les informations fournies sont correctes et, si tel est le cas, génère le certificat et vous le renvoie.

On peut comparer un certificat X.509 à un certificat sur papier standard (similaire à celui que vous avez pu recevoir au terme d'une formation de secouriste) avec une clé publique. Il contient votre nom, des informations vous concernant, ainsi que la signature de l'émetteur.

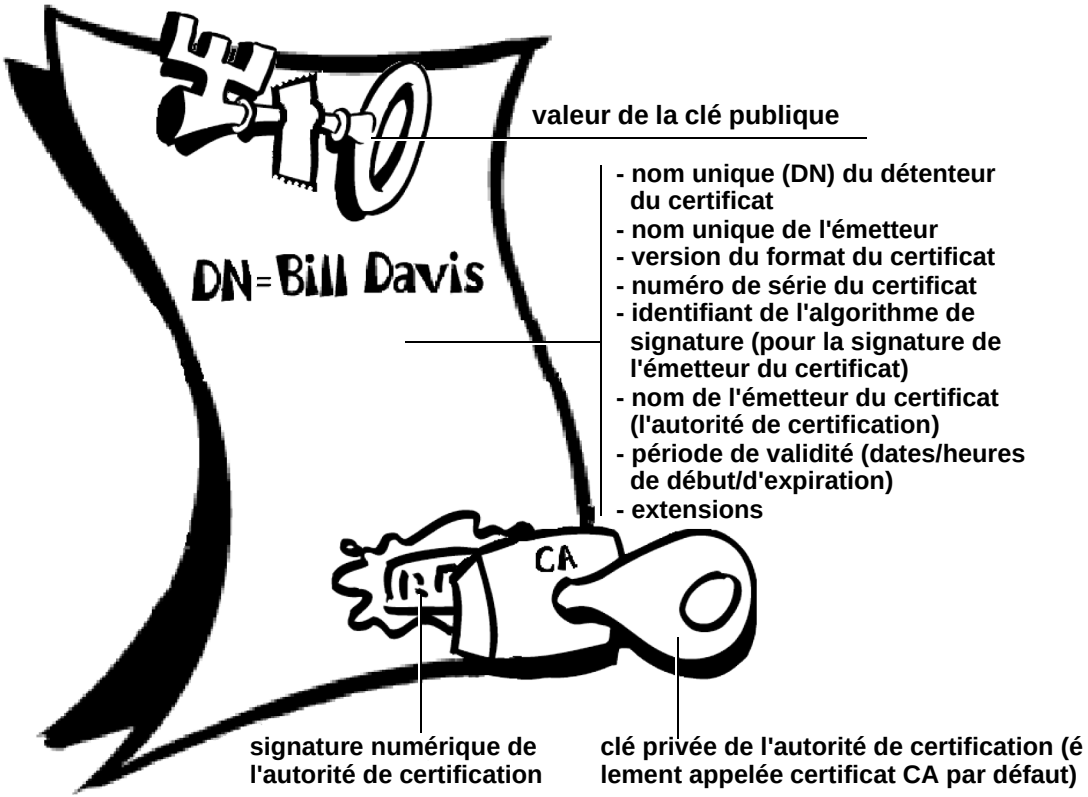

Figure 1-10. Un certificat X.509

C'est probablement au niveau des navigateurs Web que l'utilisation des certificats X.509 a été la plus systématique et la plus évidente.

Validité et fiabilité

Dans un système de clés publiques, chaque utilisateur risque de confondre une fausse clé (certificat) avec une clé authentique. La *validité* garantit qu'un certificat de clé publique appartient bien à la personne se présentant comme son détenteur. La validité est essentielle dans un environnement de clés publiques dans lequel il faut constamment vérifier l'authenticité de chaque certificat.

Lorsque vous êtes assuré de la validité d'un certificat appartenant à une personne, vous pouvez signer la copie sur votre trousseau de clés local, afin d'attester que vous avez vérifié le certificat et son authenticité. Si vous souhaitez communiquer aux autres utilisateurs que vous avez approuvé ce certificat, vous pouvez exporter la signature vers un serveur de certificats, afin qu'elle soit visible par tous.

Comme le décrit la section « Infrastructures de clé publique », certaines entreprises désignent une ou plusieurs autorités de certification (CA) pour indiquer la validité du certificat. Dans une société utilisant une PKI avec des certificats X.509, il incombe à la CA d'*émettre* des certificats à l'attention des utilisateurs (procédé qui implique généralement une réponse à la demande de certificat d'un utilisateur). Dans une société utilisant des certificats PGP sans PKI, le rôle de la CA est de vérifier l'authenticité de tous les certificats PGP, puis de les signer. En fait, une CA vise principalement à associer une clé publique aux informations d'identification contenues dans le certificat et ainsi d'assurer aux tiers que des mesures de sécurité ont été prises pour garantir la validité de cette association.

Dans une société, la CA est le « grand manitou » de la validation, une personne de confiance. Et dans certaines sociétés, telles que celles utilisant une PKI, un certificat est considéré comme valide uniquement lorsqu'il a été signé par une CA de confiance.

Vérification de la validité

Vous pouvez établir la validité manuellement et ce, de plusieurs manières. Vous pouvez demander à votre destinataire de vous remettre physiquement une copie de sa clé publique. Cependant, cette méthode peut s'avérer peu pratique et inefficace.

Vous pouvez également procéder à une vérification manuelle de l'*empreinte digitale* du certificat. L'empreinte digitale de chaque certificat PGP est unique, tout comme les empreintes digitales d'un individu. L'empreinte digitale est un hachage du certificat de l'utilisateur et constitue l'une des propriétés du certificat. Dans PGP, elle peut être un nombre hexadécimal ou une série de *mots biométriques*, phonétiquement distincts et employés pour faciliter le processus d'identification.

Vous pouvez vérifier la validité d'un certificat en appelant le détenteur de la clé (vous débutez ainsi la transaction) et en l'invitant à lire l'empreinte digitale de sa clé pour vérifier son authenticité. Cette méthode fonctionne si vous connaissez la voix du détenteur. Mais comment est-il possible de vérifier manuellement l'identité d'une personne que vous ne connaissez pas ? C'est la raison pour laquelle certaines personnes inscrivent l'empreinte digitale de leur clé sur leurs cartes de visite.

Une autre manière d'établir la validité du certificat d'un utilisateur est *de faire confiance* au tiers qui a effectué le processus de validation.

Par exemple, une CA se doit de vérifier que la partie de clé publique appartient bien au détenteur supposé avant d'émettre un certificat. Toute personne faisant confiance à la CA considère alors que tous les certificats signés par cette CA sont valides.

Un autre aspect de la vérification de la validité consiste à garantir la non révocation du certificat. Pour plus d'informations, reportez-vous à la section « Révocation de certificats ».

Etablissement de la fiabilité

Vous validez des *certificats* et faites confiance à des *utilisateurs*. En termes plus précis, vous faites confiance à certaines personnes afin qu'elles valident les certificats d'autres personnes. A moins que le détenteur du certificat ne vous remette ce dernier en mains propres, vous devez généralement vous fier à la parole d'autrui.

Gestionnaires en chef de la sécurité et correspondants fiables

En règle générale, la CA inspire une confiance totale pour établir la validité des certificats et effectuer tout le processus de validation manuelle. Cette procédure est appropriée pour un nombre défini d'utilisateurs ou de postes de travail. Au-delà de cette limite, la CA ne peut pas conserver le même niveau de qualité de validation. Dans ce cas, l'intervention d'autres validateurs s'avère nécessaire.

Une CA peut également désigner *un gestionnaire en chef de la sécurité*. Outre la validité des clés, un gestionnaire en chef de la sécurité définit également leur *fiabilité*. De la même manière qu'un souverain confie son sceau à ses conseillers afin que ces derniers agissent en son nom, le gestionnaire en chef de la sécurité permet à d'autres utilisateurs d'agir en tant que *correspondants fiables*. Ces correspondants fiables peuvent procéder à la validation des clés de la même manière que le gestionnaire en chef de la sécurité. Ils ne peuvent toutefois pas créer de nouveaux correspondants fiables.

Les termes « gestionnaire en chef de la sécurité » et « correspondant fiable » sont propres à PGP. Dans un environnement X.509, le gestionnaire en chef de la sécurité et les correspondants fiables sont respectivement appelés *Autorité de certification par défaut* (CA par défaut) et *Autorités de certification* subordonnées.

La CA par défaut utilise la clé privée associée à un type de certificat spécial, appelé *certificat CA par défaut*, afin de signer les certificats. Tout certificat signé par le certificat CA par défaut est considéré comme valide par tout autre certificat signé par défaut. Ce processus de validation fonctionne également pour les certificats signés par d'autres CA du système, à condition que le certificat de CA par défaut ait signé le certificat de CA subordonnée. En outre, tout certificat signé par la CA est considéré comme valide par les autres certificats de la hiérarchie. Ce processus de contrôle du système visant à déterminer les signataires des certificats est appelé suivi du *chemin de certification* ou d'une *chaîne de certification*.

Modèles de fiabilité

Dans des systèmes relativement fermés, par exemple au sein d'une petite entreprise, il est facile de suivre le chemin de certification jusqu'à la CA par défaut. Cependant, les utilisateurs doivent souvent communiquer avec des personnes externes à leur entreprise, qu'ils n'ont parfois jamais rencontrées, telles que des fournisseurs, des clients, des associés, etc. Il est difficile d'établir une ligne de confiance avec les personnes n'ayant pas été explicitement considérées comme fiables par votre CA.

Les entreprises suivent un *modèle de fiabilité* définissant la manière dont les utilisateurs établissent la validité des certificats. Il existe trois modèles de fiabilité différents :

- Fiabilité directe
- Fiabilité hiérarchique
- Fiabilité du Web

Fiabilité directe

La fiabilité directe est le modèle de fiabilité le plus simple. Dans ce modèle, un utilisateur est sûr qu'une clé est valide parce qu'il en connaît la provenance. Tous les systèmes de cryptographie utilisent cette forme de fiabilité d'une façon ou d'une autre. Par exemple, dans les navigateurs Web, les clés de l'autorité de certification par défaut disposent d'une fiabilité directe, car elles ont été envoyées par le fabricant. S'il existe une forme quelconque de hiérarchie, elle se décline à partir de ces certificats à fiabilité directe.

Dans PGP, un utilisateur qui valide les clés lui-même et ne désigne jamais un autre certificat comme correspondant fiable utilise la fiabilité directe.

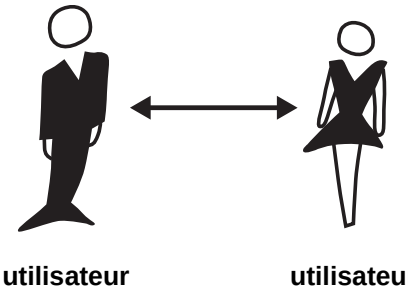

Figure 1-11. Fiabilité directe

Fiabilité hiérarchique

Dans un système hiérarchique, il existe un certain nombre de certificats « par défaut » sur lesquels se fonde la fiabilité. Ces certificats peuvent directement certifier d'autres certificats ou certifier des certificats qui en certifient d'autres, et ainsi de suite. On peut comparer cette structure à un grand « arbre » de fiabilité. La validité du certificat « feuille » est vérifiée en remontant vers le certificat qui l'a rendu fiable, puis vers d'autres certificats ayant rendu fiable ce dernier et enfin d'autres le précédant, jusqu'à atteindre le certificat par défaut à fiabilité directe.

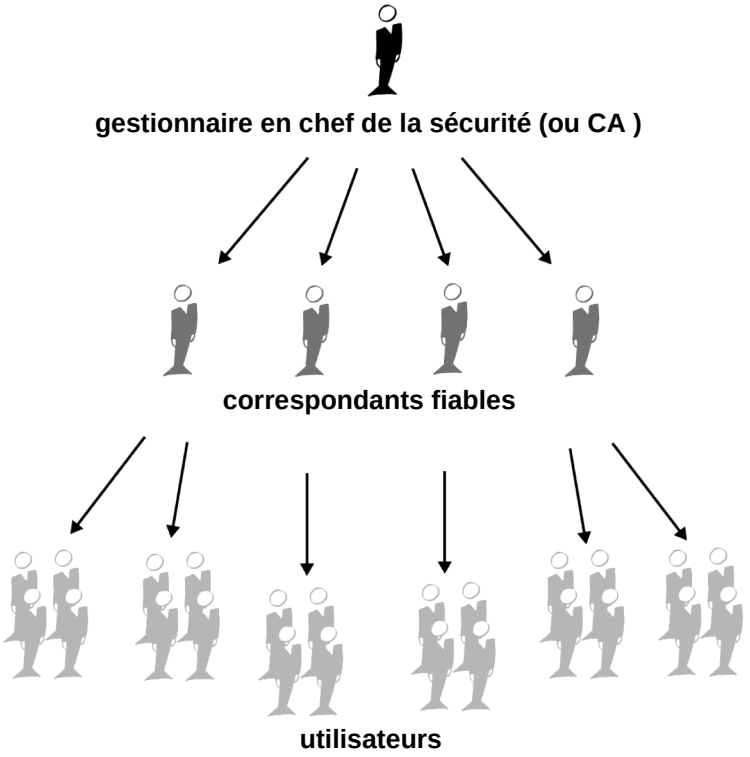

Figure 1-12. Fiabilité hiérarchique

Fiabilité du Web

La fiabilité du Web comprend les deux modèles précédents, mais ajoute également la notion selon laquelle la fiabilité dépend de l'opinion de l'utilisateur (qui a une vue réaliste) et l'idée que plus on dispose d'informations, mieux c'est. Il s'agit donc d'un modèle de fiabilité cumulatif. Un certificat peut être rendu fiable directement ou par une chaîne remontant vers un certificat par défaut à fiabilité directe (le gestionnaire en chef de la sécurité) ou par un groupe de correspondants.

Peut-être avez-vous déjà entendu parler du concept des *six degrés de séparation*, selon lequel une personne, où qu'elle se trouve, peut définir un lien avec une toute autre personne via un maximum de six autres personnes jouant le rôle d'intermédiaires. Il s'agit d'un réseau de correspondants.

Cette notion de fiabilité est également celle de PGP. PGP utilise des signatures numériques comme forme de présentation. Lorsqu'un utilisateur signe la clé d'un autre, il devient un correspondant de cette clé. Ce processus, lorsqu'il fonctionne, établit une *fiabilité du Web.*

Dans un environnement PGP, *tout* utilisateur peut agir en tant qu'autorité de certification. Il peut donc valider le certificat de clé publique d'un autre utilisateur PGP. Cependant, un tel certificat peut être considéré comme valide par un autre utilisateur uniquement si un tiers reconnaît celui qui a validé ce certificat comme un correspondant fiable. C'est-à-dire, si l'on respecte par exemple mon opinion selon laquelle les clés des autres sont correctes uniquement si je suis considéré comme un correspondant fiable. Dans le cas contraire, mon opinion sur la validité d'autres clés est controversée.

Des indicateurs stockés sur le trousseau de clés publiques de chaque utilisateur permettent de :

- Définir si l'utilisateur considère une clé spécifique comme correcte
- Déterminer le niveau de fiabilité que l'utilisateur attribue à la clé afin que le détenteur de cette clé puisse en certifier d'autres

Indiquez, par exemple sur votre copie de ma clé, si vous pensez que mon jugement est à prendre en compte ou non. Il s'agit réellement d'un système de réputation : certaines personnes sont réputées donner des signatures correctes et les autres utilisateurs leur font confiance lorsqu'elles valident d'autres clés.

Niveaux de fiabilité dans PGP

Le niveau maximal de fiabilité d'une clé, la confiance *implicite*, est la confiance en votre propre paire de clés. PGP part du principe que si vous possédez la clé privée, vous devez faire confiance aux opérations liées à la clé publique associée. Toutes les clés signées par votre clé rendue fiable implicitement sont valides.

Vous pouvez affecter trois niveaux de fiabilité à la clé publique d'un autre utilisateur :

- *Fiabilité* complète
- *Fiabilité* marginale
- *Non fiable*

Bien sûr, pour ne pas simplifier les choses, il existe également trois niveaux de validité :

- Valide
- Correcte de manière marginale
- Incorrect

Pour définir la clé d'un autre utilisateur comme correspondant fiable :

1. Commencez avec une clé valide signée
   - par vous-même ou par
   - un autre correspondant fiable,

   puis
2. définissez le niveau de fiabilité auquel a droit le détenteur de la clé.

Supposons, par exemple, que votre trousseau de clés contient la clé d'Alice. Vous l'avez validée et, pour l'indiquer, vous la signez. En outre, vous savez qu'Alice est très pointilleuse en ce qui concerne la validation des clés d'autres utilisateurs. Par conséquent, vous affectez une fiabilité complète à sa clé. Alice devient ainsi une autorité de certification. Si elle signe la clé d'un autre utilisateur, cette clé apparaît comme valide sur votre trousseau de clés.

Pour définir une clé comme valide, PGP exige une signature à fiabilité complète ou deux signatures à fiabilité marginale. Cette exigence est similaire à celle d'un vendeur qui vous demande deux pièces d'identité. Vous pouvez penser qu'Alice et Robert sont dignes de confiance. Chacun d'eux peut malencontreusement signer une fausse clé, aussi ne devez-vous pas considérer l'un d'eux comme étant complètement fiable. Toutefois, le risque qu'Alice et Robert signent cette même clé est minime.

Révocation de certificats

Les certificats sont utiles tant qu'ils sont valides. Si vous considérez que la validité d'un certificat est permanente, la sécurité n'est plus garantie. Dans la plupart des entreprises et dans toutes les infrastructures de clé publique, les certificats ont une durée de vie limitée. Par conséquent, en cas de compromis de certificat, la période de vulnérabilité d'un système est réduite.

Les certificats sont donc créés avec une *période de validité* par défaut : une date / heure de début et une date / heure d'expiration. Ce certificat peut être utilisé pendant la totalité de sa période de validité (sa *durée de vie*). Lorsque ce certificat arrive à expiration, il n'est plus valide, car l'authenticité de sa paire de clés / d'identification n'est plus assurée. Même si vous pouvez l'utiliser en toute sécurité pour reconfirmer les informations cryptées ou signées pendant la période de validité, vous ne devez pas le considérer comme fiable pour les tâches cryptographiques à venir.

L'annulation d'un certificat préalablement à sa date d'expiration peut parfois s'avérer nécessaire, en particulier lorsque son détenteur quitte l'entreprise ou pense que la clé privée correspondante est compromise. Dans ce cas, on parle de *révocation*. Vous devez considérer un certificat révoqué avec *bien plus* de suspicion qu'un certificat arrivé à expiration. Les certificats expirés sont inutilisables, mais ne constituent pas une menace aussi sérieuse pour la sécurité que les certificats révoqués.

Toute personne ayant signé un certificat peut révoquer sa signature (à condition qu'elle utilise la même clé privée que celle employée pour la création de la signature). Une signature révoquée indique soit que le signataire ne croit plus que les informations d'identification correspondent à la clé publique, soit que la clé publique du certificat (ou la clé privée correspondante) est compromise. Une signature révoquée doit être presque aussi importante qu'un certificat révoqué.

Pour les certificats X.509, une signature révoquée est pratiquement équivalente à un certificat révoqué, car la seule signature présente sur le certificat est celle l'ayant rendu valide, à savoir la signature de la CA. Les certificats vous permettent en outre de révoquer la totalité de votre certificat (pas uniquement les signatures qu'il contient) si vous pensez qu'il est compromis.

Seul le détenteur du certificat (le détenteur de sa clé privée correspondante) ou un autre utilisateur, *désigné* comme autorité de révocation par le détenteur du certificat, a la possibilité de révoquer un certificat PGP. La désignation d'une autorité de révocation est utile, car la révocation, par un utilisateur PGP, de son certificat est souvent due à la perte du mot de passe complexe de la clé privée correspondante. Or, cette procédure peut uniquement être effectuée s'il est possible d'accéder à la clé privée. Un certificat X.509 peut uniquement être révoqué par son émetteur.

Communication de la révocation d'un certificat

Lorsqu'un certificat est révoqué, il est important d'en avertir ses utilisateurs potentiels. Pour informer de la révocation des certificats PGP, la méthode habituelle consiste à placer cette information sur un serveur de certificats. Ainsi, les utilisateurs souhaitant communiquer avec vous sont avertis de ne pas utiliser cette clé publique.

Dans un environnement PKI, vous êtes généralement informé sur les certificats révoqués via une structure de données appelée *Liste de révocation des certificats*, ou *LRC*, publiée par la CA. Cette LRC contient une liste validée et horodatée de tous les certificats révoqués et non expirés du système. Les certificats révoqués figurent sur la liste jusqu'à leur expiration, puis ils sont supprimés pour ne pas surcharger la liste.

La CA distribue la LRC aux utilisateurs à intervalles réguliers (et éventuellement hors cycle, à savoir lors de la révocation d'un certificat) afin de les empêcher, en théorie, d'utiliser sans le savoir un certificat compromis. Toutefois, il peut arriver qu'un nouveau certificat compromis soit utilisé entre deux LRC différentes.

Qu'est-ce qu'un mot de passe complexe ?

La plupart des utilisateurs connaissent parfaitement la procédure de restriction d'accès aux systèmes informatiques via un *mot de passe*, une chaîne de caractères unique entrée par un utilisateur pour permettre son identification.

Un *mot de passe complexe* est plus long et théoriquement plus sécurisé qu'un mot de passe habituel. Généralement composé de plusieurs mots, il est plus sécurisé contre les *attaques « au dictionnaire »* standard, où le pirate tente d'entrer tous les mots du dictionnaire afin de deviner votre mot de passe. Les meilleurs mots de passe complexes sont relativement longs et invulnérables, car ils contiennent une combinaison de majuscules et de minuscules, des nombres et des signes de ponctuation.

PGP utilise un mot de passe complexe pour le cryptage de votre clé privée sur votre ordinateur. Votre clé privée est cryptée sur votre disque en utilisant un hachage de votre mot de passe complexe comme clé secrète. Vous utilisez le mot de passe complexe pour le décryptage et l'utilisation de votre clé privée. Il doit être facile à mémoriser, mais les autres utilisateurs ne doivent pas pouvoir le deviner. Plutôt que de l'inventer, il est préférable d'en choisir un ancré dans votre esprit. Pourquoi ? Parce que **si vous oubliez votre mot de passe complexe, vous perdez vos données**. Votre clé privée ne sert strictement à rien sans votre mot de passe complexe, et vous ne pouvez plus rien faire. Vous n'avez pas oublié la citation du début de ce chapitre ? PGP est une cryptogra-

phie permettant même de sécuriser vos fichiers contre les gouvernements les plus puissants. Il protègera également sans nul doute vos fichiers contre vous-même. En effet, n'oubliez jamais ce point si vous décidez de remplacer votre mot de passe complexe par la chute de la fameuse blague dont vous ne vous souvenez presque jamais.

Découpage de clé

Selon l'expression populaire, un secret partagé n'est plus un secret. C'est le problème du partage d'une paire de clés privées. Même s'il n'est pas recommandé, le partage d'une paire de clés privées s'avère parfois nécessaire. Les *clés de signature d'entreprise*, par exemple, sont des clés privées utilisées par une entreprise pour la signature, entre autres, de documents juridiques, d'informations personnelles confidentielles ou de communiqués de presse afin d'authentifier leur origine. Dans ce cas, il peut être utile de permettre à plusieurs salariés d'une entreprise d'accéder à la clé privée. Toutefois, ceci signifie que chaque salarié peut agir au nom de l'entreprise.

Il est donc conseillé de *découper* cette clé entre plusieurs personnes, de sorte que chacune d'elles doive présenter sa partie de la clé afin de la reconstituer et de pouvoir l'utiliser. Si trop de pièces sont manquantes, la clé est inutilisable.

Vous pouvez, par exemple, découper une clé en trois parties et en exiger deux pour la reconstituer, ou la découper en deux parties et exiger chacune d'elles. Si vous utilisez une connexion réseau sécurisée lors du processus de reconstitution, il n'est pas nécessaire que les détenteurs d'une partie de la clé soient présents pour assembler cette clé.

Détails techniques

Ce chapitre fournit une présentation détaillée des concepts et de la terminologie cyptographiques. Dans le Chapitre 2, Phil Zimmermann, créateur de PGP, explique de façon approfondie le concept de confidentialité, les détails techniques relatifs au fonctionnement de PGP, y compris les algorithmes utilisés, ainsi que les diverses attaques et les modes de protection possibles.

Pour plus d'informations sur la cryptographie, reportez-vous aux ouvrages mentionnés dans la section « Lectures annexes » de la préface.

Phil Zimmermann à propos de PGP 2

Ce chapitre comporte des données de base à la fois sur la cryptographie et sur PGP, telles que fournies par Phil Zimmermann.

Pourquoi ai-je créé PGP ?

« Quoi que vous fassiez, cela sera de peu d'importance, mais il est fondamental que vous le réalisiez. »
—Mahatma Gandhi.

C'est personnel et privé. Et cela ne regarde personne d'autre que vous. Vous pouvez être en train de préparer une campagne politique, de parler de vos impôts ou de vivre une idylle secrète. Vous pouvez également être en relation avec un dissident politique victime des méthodes répressives de son pays. Quel que soit le sujet, vous ne souhaitez pas que vos messages électroniques personnels (e-mail) ou que vos documents confidentiels soient lus par quiconque. Vous avez le droit de vouloir protéger votre vie privée. C'est aussi simple que la Constitution américaine.

Le droit de protéger sa vie privée est énoncé implicitement dans l'ensemble de la Déclaration des droits des citoyens. Cependant, lors de l'élaboration de la Constitution américaine, les Pères fondateurs n'ont pas jugé nécessaire de formuler explicitement le droit d'avoir une conversation privée. Cela aurait été ridicule, car, il y a deux cents ans, toutes les conversations pouvaient se dérouler en privé. Si une personne était à proximité, il suffisait d'aller derrière la grange, puis de continuer à converser. Personne ne pouvait vous écouter à votre insu. Le droit d'avoir une conversation confidentielle relevait des droits naturels, pas uniquement au sens philosophique du terme mais aussi au sens physique en raison du niveau de technologie de l'époque.

L'invention du téléphone, qui a marqué le début de l'ère de l'information, a tout révolutionné. Aujourd'hui, la plupart de nos conversations sont véhiculées électroniquement. Aussi, les plus intimes peuvent être écoutées sans que nous le sachions. Un téléphone portable peut être contrôlé par quiconque dispose d'une radio. Les messages électroniques envoyés via Internet ne sont pas plus sécurisés que les appels passés par téléphone portable. Aujourd'hui, l'e-mail remplace de plus en plus le courrier postal et, à mesure qu'il perd de son aspect novateur, il devient la norme d'échange d'informations utilisée par tous. L'e-mail peut être régulièrement et automatiquement analysé à grande échelle dans le but de rechercher des mots clés intéressants sans que cela soit détecté. Cela ressemble à la pêche aux filets dérivants.

Vous pensez peut-être que le cryptage de vos e-mails ne se justifie pas. Si vous êtes réellement un citoyen respectueux de la loi et n'ayant rien à cacher, pourquoi ne pas envoyer systématiquement votre courrier écrit sur carte postale ? Pourquoi ne pas se soumettre à des contrôles anti–dopage sur demande ? Pourquoi exiger un mandat de perquisition à la police se présentant chez vous ? Cherchez-vous à cacher quelque chose ? Si vous dissimulez votre courrier dans des enveloppes, cela signifie-t-il que vous êtes un esprit subversif, un trafiquant de drogue ou même un paranoïaque ? Les citoyens respectueux des lois doivent–ils crypter leurs e-mails ?

Que se passerait-il si nous pensions tous que les citoyens en règle devaient utiliser des cartes postales pour leur courrier ? Si une personne non conformiste faisait valoir le droit à la protection de la vie privée en utilisant une enveloppe pour son courrier, cela éveillerait les soupçons. Les autorités pourraient ouvrir son courrier afin de découvrir ce qu'elle cherche à dissimuler. Heureusement, nous ne vivons pas dans ce type d'univers et nous cachons presque toutes nos missives à l'aide d'enveloppes. Aussi, personne n'attire de soupçons en protégeant sa vie privée de cette manière. C'est la vérité du plus grand nombre. De la même manière, il serait bien commode que chacun prenne l'habitude de crypter l'ensemble de ses e-mails, innocents ou non, car le recours à une telle pratique n'éveillerait pas les soupçons. Vous pouvez considérer cette démarche comme une forme de solidarité.

Jusqu'à présent, si le gouvernement souhaitait violer la vie privée de citoyens landa, il devait consacrer beaucoup d'argent et d'efforts pour intercepter, ouvrir à la vapeur, puis lire une lettre. Il devait également écouter et éventuellement transcrire des conversations téléphoniques, du moins jusqu'à l'apparition de la technologie de reconnaissance vocale. Ce type de contrôle laborieux était peu commode à grande échelle. Il était utilisé uniquement lorsque c'était jugé nécessaire.

Le projet de loi sénatoriale américaine 266 datant de 1991 et ayant pour objet de lutter contre toutes les formes d'infractions comportait une mesure troublante. Si cette résolution non impérative était entrée en vigueur, elle aurait contraint les fabricants d'équipements de communications sécurisés à insérer dans leurs produits des « trappes » spéciales de manière à ce que le gouvernement puisse lire les messages cryptés de tout un chacun. Elle stipule que « Le Congrès a pour intention de demander aux prestataires et aux fabricants d'équipements de services de communication électronique de garantir que les systèmes de communication permettent au gouvernement d'obtenir le texte en clair du contenu des communications vocales, de données et autres, lorsque la loi l'autorise. » C'est ce projet de loi qui m'a incité, cette année là, à proposer la publication électronique gratuite de PGP, peu de temps avant que cette mesure législative ne soit abandonnée suite aux vigoureuses protestations des groupes industriels et des défenseurs des libertés individuelles.

La loi américaine sur la téléphonie numérique votée en 1994 (Digital Telephony bill) a imposé l'installation par les opérateurs de ports d'écoute téléphonique distants dans leurs commutateurs numériques, créant par là même une nouvelle infrastructure technologique pour l'écoute téléphonique « pointer-et-cliquer ». Ainsi, les agents fédéraux ne sont plus obligés de sortir pour fixer des pinces crocodiles aux lignes téléphoniques. Ils peuvent désormais écouter vos appels téléphoniques à partir de leur quartier général à Washington. Naturellement, la loi exige toujours un mandat pour procéder à une écoute. Cependant, alors que les infrastructures technologiques peuvent rester en l'état pendant des décennies, les lois et les politiques peuvent changer du jour au lendemain. Lorsqu'une infrastructure de communications optimisée pour la surveillance est solidement établie, une modification du paysage politique peut aboutir à des abus. L'élection d'un nouveau gouvernement ou, cas extrême, le bombardement d'un bâtiment du gouvernement fédéral, peut modifier le contexte politique.

Un an après le vote, en 1994, de la loi sur la téléphonie numérique, le FBI a rendu public le projet visant à demander aux opérateurs téléphoniques d'intégrer dans leur infrastructure la capacité de capter simultanément 1 pour cent des conversations téléphoniques dans les principales villes des Etats-Unis. Cela équivaut à la multiplication par plus de 1 000 du nombre de mises sur écoute. Auparavant, seuls quelque mille écoutes téléphoniques par an étaient effectuées sur mandat aux Etats-Unis, à la fois aux niveaux local, fédéral et étatique. Il est non seulement difficile d'imaginer comment le gouvernement pourrait employer suffisamment de juges pour signer le nombre de mandats permettant de procéder à l'écoute de 1 pour cent des appels téléphoniques des Américains, mais il est encore plus difficile de concevoir comment il pourrait recruter assez d'agents fédéraux pour rester assis à les écouter en temps réel. La seule manière plausible de traiter ces appels requerrait une application digne d'Orwell de la technologie de reconnaissance vocale automatique pour passer au crible toutes les conversations à la recherche de mots clés intéressants ou de voix particulières. Si le gouvernement ne détecte pas sa cible parmi ce premier échantillon, les écoutes peuvent être effectuées sur un autre échantillon de la même taille jusqu'à ce que la recherche soit fructueuse ou encore jusqu'à ce que chaque ligne téléphonique ait été contrôlée pour circulation d'informations subversives. Le FBI a déclaré qu'une telle procédure serait nécessaire dans le futur. Ce projet provoqua une telle indignation qu'il fut rejeté par le Congrès, en tous les cas cette fois-ci, en 1995. Néanmoins, une telle demande du FBI pour obtenir de plus larges pouvoirs est révélatrice de ses intentions futures. L'échec de ce projet n'est pas particulièrement rassurant lorsque l'on pense que la loi sur la téléphonie numérique de 1994 avait été rejetée lors de sa première présentation en 1993.

Les progrès réalisés dans le domaine de la technologie ne permettront pas le maintien du statu quo en matière de confidentialité. Ce statu quo est instable. Si nous n'agissons pas, les nouvelles technologies fourniront au gouvernement de nouvelles possibilités de surveillance automatique auxquelles Staline n'aurait même pas pu rêver. Le recours à la cryptographie invulnérable constitue la seule manière de protéger la confidentialité des lignes téléphoniques en pleine ère de l'information.

Ce recours à la cryptographie ne doit pas être motivé par une méfiance vis-à-vis du gouvernement. Votre société peut être mise sur écoute par vos concurrents, par le grand banditisme ou par des gouvernements étrangers. Ainsi, plusieurs gouvernements étrangers reconnaissent faire appel à leurs services de renseignements pour l'espionnage des sociétés étrangères afin de fournir à leurs propres entreprises un avantage concurrentiel. Ironie du sort, les restrictions imposées par le gouvernement américain en matière de cryptographie ont affaibli le système de défense des entreprises américaines contre les services de renseignements étrangers et le grand banditisme.

Le gouvernement est conscient du rôle clé que la cryptographie jouera dans ses relations avec la population. En avril 1993, l'administration de Clinton a rendu public une toute nouvelle initiative de politique de cryptage étudiée par l'agence de sécurité nationale américaine (National Security Agency - NSA) depuis l'arrivée de Bush à la présidence. La pièce maîtresse de cette initiative consistait en un système de cryptage conçu par les autorités, appelé la puce Clipper, contenant un nouvel algorithme de cryptage NSA classifié. Le gouvernement a essayé d'encourager l'industrie du secteur privé à l'intégrer dans l'ensemble de ses produits de communication sécurisés, tels que les téléphones et télécopieurs sécurisés, etc. AT&T a incorporé le système Clipper dans ses produits sécurisés impliquant l'usage de la voix. Voici ce qui se cache derrière ce système : pendant tout le processus de fabrication, chaque puce Clipper est chargée avec sa propre et unique clé dont le gouvernement obtient une copie placée en dépôt. Cependant, ne soyez pas inquiets, le gouvernement a promis qu'il utiliserait ces clés pour lire vos conversations uniquement « lorsque dûment habilité par la loi ». Naturellement, pour donner au système Clipper toute son efficacité, une mesure consistant à proscrire toute autre forme de cryptographie doit s'ensuivre.

Le gouvernement a commencé par déclarer que le recours au système Clipper serait volontaire et non imposé, contrairement à d'autres types de cryptographie. Cependant, la réaction de la population contre l'usage de cette puce a été plus forte que ne l'auraient imaginée les autorités. L'industrie informatique a unanimement exprimé son opposition à l'utilisation du système Clipper.
Le Directeur du FBI, Louis Freeh, a affirmé au cours d'une conférence de presse en 1994 que si ce système ne parvenait pas à obtenir le soutien du public et que si les services d'écoute du FBI perdaient leur raison d'être en raison d'une cryptographie contrôlée par le gouvernement, ses services auraient comme dernier recours d'ester en justice pour réclamer des dommages et inté-

rêts. Suite à la tragédie d'Oklahoma City, M. Freeh a déclaré au cours de son témoignage devant le Comité judiciaire du Sénat que le gouvernement se devait de limiter les possibilités de recours parmi la population à la cryptographie invulnérable (bien que personne n'ait suggéré que les terroristes l'aient utilisée).

Le centre américain d'informations luttant pour les libertés individuelles sur les réseaux informatiques (The Electronic Privacy Information Center - EPIC) a eu connaissance de documents révélateurs dans le cadre de la loi sur la liberté d'information (Freedom of Information Act). Dans un document intitulé « Cryptage : menaces, applications et solutions éventuelles » envoyé au Conseil américain de la sécurité nationale en février 1993, au FBI, à la NSA et au Département de la justice (Department of justice - DOJ), il est conclu que « les solutions techniques, telles qu'elles se présentent actuellement, sont exploitables uniquement si elles sont intégrées à l'ensemble des produits de cryptage. Pour ce faire, il est nécessaire d'élaborer un texte législatif requérant l'utilisation de produits de cryptage agréés par le gouvernement ou respectant les exigences gouvernementales en matière de cryptage. »

Les antécédents du gouvernement quant au respect total des libertés individuelles des citoyens n'inspirent pas confiance. Le programme COINTELPRO du FBI visait des groupes d'opposants à la politique gouvernementale. Le FBI a espionné les mouvements pacifistes et ceux défendant les droits des citoyens. Il a mis sur écoute téléphonique Martin Luther King Jr. ; Nixon tenait une liste de ses ennemis. Sur ces entrefaites, le scandale du Watergate éclata. Le Congrès semble aujourd'hui résolu à voter des lois réduisant nos libertés individuelles sur Internet. Jamais depuis le début du siècle la méfiance de la population vis-à-vis du gouvernement n'avait à ce point envahi le monde politique, toutes tendances confondues.

L'une des manières de lutter contre la tendance inquiétante du gouvernement à considérer la cryptographie comme illicite consiste à employer à cette technique autant que possible tant qu'elle reste légale. Une fois l'utilisation récurrente de la cryptographie invulnérable entrée dans les mœurs, il deviendra plus difficile pour les autorités de la réprimander. C'est pourquoi l'utilisation de PGP sert la démocratie.

Si la protection de la vie privée devient illégale, seuls les hors-la-loi pourront bénéficier d'intimité. Les organismes de renseignements disposent de technologies de cryptage de haut niveau, au même titre que les grands trafiquants de drogue et d'armes. Toutefois, de nos jours le citoyen landa et les organisations politiques de base n'ont généralement pas accès à la technologie cryptographique de clés publiques bon marché de « standard militaire ». Mais demain…

PGP donne à chacun le pouvoir de prendre en main sa vie privée. Je l'ai créé pour répondre au besoin ressenti par une grande partie de la société.

Les algorithmes symétriques de PGP

PGP propose une sélection de plusieurs algorithmes de clés secrètes afin de crypter le message réel. Par algorithme de clé secrète, nous désignons un chiffrement par bloc conventionnel ou symétrique utilisant la même clé pour le cryptage et le décryptage. Les trois chiffrements par bloc symétriques offerts par PGP sont CAST, DES triple et IDEA. Il ne s'agit pas d'algorithmes « faits maison », mais tous ont été développés par des équipes d'éminents cryptographes.

Pour ceux s'intéressant de près à la cryptographie, qu'ils sachent que les trois chiffrements fonctionnent sur des blocs de texte en clair et chiffré de 64 bits. La taille des clés CAST et IDEA atteint 128 bits et celle de DES triple, 168 bits. A l'instar de DES (Data Encryption Standard), un de ces chiffrements peut être utilisé en mode de renvoi de chiffrement (Cipher Feedback - CFB) et de chaînage de blocs de chiffrement (Cipher Block Chaining - CBC). Sur PGP, ils fonctionnent en mode CFB 64 bits.

J'ai inclus l'algorithme de cryptage de CAST dans PGP, car ce chiffrement par bloc présente l'avantage de comporter une clé de 128 bits, d'être rapide et gratuit. Son nom est composé des initiales de ses inventeurs, à savoir Carlisle Adams et Stafford Tavares de Northern Telecom (Nortel). Nortel a présenté une demande de brevet pour CAST, mais s'est engagé par écrit à fournir CAST à quiconque sans versement de droits. CAST semble avoir été particulièrement bien conçu par des personnes jouissant d'une bonne réputation dans ce domaine. Cette conception repose sur un ensemble d'affirmations pouvant être formellement démontrées et laissant à penser qu'un nombre impressionnant de clés est nécessaire pour casser sa clé de 128 bits. CAST ne comporte aucune clé faible ou semi-faible. De nombreux éléments tangibles tendent à montrer l'immunité totale de CAST contre la cryptanalyse linéaire et différentielle, les formes de cryptanalyse les plus performantes répertoriées dans la littérature disponible dans le domaine et qui ont été à même de casser DES. CAST est trop récent pour qu'un dossier d'antécédents exhaustif soit constitué, mais sa conception formelle et la bonne réputation de ses inventeurs attireront indubitablement l'attention et les critiques du reste de la communauté cryptographique académique. J'éprouve quasiment le même sentiment de confiance vis-à-vis de CAST que d'IDEA, le chiffrement que j'avais sélectionné pour des versions plus récentes de PGP il y a quelques années. A cette époque, IDEA était également trop récent pour constituer un dossier d'antécédents, mais il a fait son chemin.

Le chiffrement par bloc IDEA (International Data Encryption Algorithm – Algorithme de cryptage de données international) est basé sur la conception consistant à « associer des opérations de différents groupes algébriques ». Il a été développé à ETH à Zurich par James L. Massey et Xuejia Lai, puis édité en 1990. Dans des publications antérieures, cet algorithme était nommé IPES (Improved Proposed Encryption Standard – Norme de cryptage proposée

améliorée), mais il a pris par la suite le nom de IDEA. Jusqu'ici, IDEA a bien mieux résisté aux attaques que d'autres chiffrements par bloc, tels que FEAL, REDOC-II, LOKI, Snefru et Khafre. Il est également plus résistant que DES vis-à-vis des attaques différentielles très puissantes que constituent Biham et Shamir, ainsi que des attaques provenant de cryptanalyse linéaire. Alors que le chiffrement continue de s'attirer les critiques des zones les plus importantes du monde cryptanalytique, la confiance en IDEA ne cesse de croître. Malheureusement, la détention du brevet pour la conception d'IDEA par Ascom Systec constitue l'obstacle majeur au passage de cet algorithme au stade de norme et, contrairement à DES et CAST, IDEA n'a pas été rendu accessible au public sans versement de droits.

PGP inclut, en guise de protection, trois clés DES triple dans son répertoire de chiffrements par bloc disponibles. DES a été développé par IBM au milieu des années 1970. Bien qu'étant bien conçu, sa clé de 56 bits est de taille insuffisante par rapport aux normes actuelles. DES triple est particulièrement invulnérable et résulte d'une étude approfondie menée sur plusieurs années. Par conséquent, il est probablement plus sûr que les nouveaux chiffrements par bloc, tels que CAST et IDEA. DES triple correspond au DES appliqué trois fois au même bloc de données, à l'aide de trois clés différentes, à l'exception près que la seconde opération DES est exécutée en arrière en mode de décryptage. DES triple est beaucoup plus lent que CAST ou IDEA, mais la rapidité importe généralement peu dans les applications e-mail. Bien que la taille de sa clé atteigne 168 bits, DES triple semble bénéficier d'une puissance de clé supérieure ou égale à 112 bits contre un pirate disposant d'une énorme capacité de stockage de données. Selon un article écrit par Michael Weiner à Crypto96, toute capacité distante potentielle de stockage de données à la disposition d'un pirate lui permettrait de lancer une attaque nécessitant quasiment autant d'efforts que pour casser une clé de 129 bits. DES triple n'est lié à aucun brevet.

Les clés publiques de PGP générées par la version 5.0, ou version ultérieure de PGP, renferment des informations indiquant au logiciel d'un expéditeur les chiffrements par bloc supportés par le logiciel du destinataire, de telle sorte qu'il sache quels chiffrements utiliser pour procéder au cryptage. Les clés publiques Diffie-Hellman / DSS acceptent CAST, IDEA ou DES triple en tant que chiffrement par bloc, CAST étant sélectionné par défaut. Pour des raisons de compatibilité, les clés RSA ne sont actuellement pas dotées de cette fonction. Seul l'algorithme IDEA est utilisé par PGP pour envoyer des messages aux clés RSA, car les versions antérieures de PGP prendraient uniquement en charge RSA et IDEA.

A propos des routines de compression de données PGP

PGP compresse habituellement le texte en clair préalablement à son cryptage. En effet il est impossible de compresser des données cryptées. Cette compression des données permet de réduire le temps de transmission du modem, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique. La plupart des techniques de cryptanalyse consistent à exploiter les redondances trouvées dans le texte en clair pour casser le chiffrement. La compression des données réduit cette redondance dans le texte en clair, améliorant ainsi considérablement la résistance à la cryptanalyse. Cette compression du texte clair prend du temps, mais la démarche en vaut la peine sur le plan de la sécurité.

PGP ne peut pas compresser les fichiers de taille insuffisante ou supportant mal ce processus. En outre, le programme reconnaît les fichiers produits par les programmes de compression les plus connus, comme PKZIP, et ne tente pas de compresser un fichier déjà compressé.

Pour ceux qui s'intéressent à la technique, le programme recourt aux routines de compression du logiciel gratuit ZIP créé par Jean-Loup Gailly, Mark Adler et Richard B. Wales. Ce logiciel utilise des algorithmes de compression fonctionnant de manière équivalente à ceux utilisés par le programme PKZIP 2.x. du logiciel PKW. Sa rapidité et son ratio de compression très performant constituent les principales raisons de la sélection du logiciel de compression ZIP pour PGP.

A propos des nombres aléatoires utilisés comme clés de session

PGP crée des clés de session temporaires à l'aide d'un générateur de nombres pseudo-aléatoires cryptographiquement invulnérable. Si ce fichier de valeurs initiales aléatoires n'existe pas, il est automatiquement créé, puis affecté de nombres véritablement aléatoires dérivés de vos événements aléatoires collectés par le programme PGP à partir de la synchronisation de vos frappes clavier et des mouvements de votre pointeur.

Ce générateur crée à nouveau le fichier de valeurs initiales aléatoires lors de chaque utilisation en y ajoutant de nouvelles données partiellement dérivées de l'heure et d'autres sources véritablement aléatoires. L'algorithme de cryptage conventionnel fait office de moteur pour le générateur de nombres aléatoires. Le fichier de valeurs initiales aléatoires contient des données et des clés aléatoires utilisées pour verrouiller le moteur de cryptage conventionnel du générateur aléatoire.

Pour diminuer les risques qu'un pirate ne dérive vos clés de la session suivante ou précédente, ce fichier doit être protégé contre toute divulgation. Le pirate aurait toutes les peines du monde à obtenir toute information utile du fichier de valeurs initiales aléatoires, car il est nettoyé cryptographiquement avant et après chaque utilisation. Néanmoins, il semble plus prudent de ne pas le mettre entre toutes les mains. Si possible, rendez ce fichier lisible par vous uniquement. Sinon, ne laissez pas n'importe qui effectuer des copies sur votre ordinateur.

A propos du résumé de message

Le résumé de message constitue un « distillat » compact (160 ou 128 bits) de la somme de contrôle de votre message ou fichier. Vous pouvez également le considérer comme une « empreinte digitale » de votre message ou fichier. Le résumé de message « représente » votre message de sorte qu'en cas d'altération du message, un autre calcul de résumé en découlerait. Cela permet de détecter toute modification apportée au message par un faussaire. Un résumé de message est calculé à l'aide d'une fonction de hachage à sens unique cryptographiquement invulnérable. D'un point de vue informatique, un pirate ne peut pas concevoir un message de substitution qui donnerait lieu à un résumé de message identique. A cet égard, un résumé de message présente plus d'avantages qu'une somme de contrôle, car il est facile de concevoir un autre message produisant la même somme de contrôle. Toutefois, ni la somme de contrôle, ni le message d'origine ne peut être dérivé(e) du résumé.

L'algorithme de résumé de message désormais utilisé par PGP (Version 5.0 et ultérieure) est nommé SHA, acronyme correspondant aux mots Secure Hash Algorithm (Algorithme de hachage sécurisé), et a été conçu par la NSA à l'attention de l'Agence gouvernementale de normes et de technologie (NIST). SHA constitue un algorithme de hachage de 160 bits. Certaines personnes éprouvent de la méfiance vis-à-vis de tout ce qui émane de la NSA, car celle-ci est chargée d'intercepter les communications et de casser les codes. N'oubliez pas que la NSA n'a aucun intérêt à falsifier des signatures et que le gouvernement bénéficierait d'une norme de signature numérique non falsifiable empêchant qui que ce soit de nier sa signature. Ceci présente des avantages divers pour l'application de la loi et la collecte de renseignements. Par ailleurs, SHA a été publié pour le grand public et a été revu dans le détail par la plupart des meilleurs cryptographes au monde spécialisés dans les fonctions de hachage. Tous reconnaissent que SHA est extrêmement bien conçu. Il comporte certaines innovations permettant de surmonter l'ensemble des faiblesses constatées dans les précédents algorithmes de résumés de message publiés par des cryptographes académiques. Toutes les nouvelles versions de PGP prennent en

charge l'algorithme de résumé de message SHA grâce auquel des signatures peuvent être créées à l'aide des nouvelles clés DSS conformes au standard de signature magnétique de la NIST. Pour des raisons de compatibilité avec les anciennes versions de PGP, les nouvelles versions de PGP prennent-elles aussi en charge RM5 pour les signatures RSA.

Le RM5, un algorithme de hachage de 128 bits, constitue l'algorithme de résumé de message utilisé par les précédentes versions de PGP. Il a été placé dans le domaine public par RSA Data Security, Inc. RM5 a failli être cassé en 1996 par le cryptographe allemand Hans Dobbertin. Cependant, bien que n'ayant pas été cassé, RM5 a révélé de telles faiblesses qu'il est déconseillé de s'en servir pour générer des signatures. En s'attelant à la tâche, il est probable qu'il puisse être entièrement cassé, permettant ainsi de falsifier des signatures. Si vous souhaitez éviter de découvrir un jour votre signature numérique PGP apposée sur une fausse déclaration, vous feriez mieux d'adopter les clés DSS de PGP comme méthode favorite pour générer des signatures numériques, car DSS utilise SHA en tant qu'algorithme de hachage sûr.

Comment protéger les clés publiques contre la falsification ?

Il n'est pas nécessaire de cacher les clés d'un système de cryptographie de clés publiques. Il est même préférable de les diffuser aussi largement que possible. Toutefois, il est important de les protéger contre la falsification afin d'être certain qu'elles appartiennent réellement aux personnes en étant à priori les détenteurs. Il peut s'agir là de la plus grande vulnérabilité affectant un système de cryptographie de clés publiques. Dans un premier temps, nous examinerons un cas de catastrophe potentielle, puis nous décrirons comment l'éviter via PGP.

Supposons que vous souhaitiez envoyer un message privé à Alice. Vous téléchargez le certificat de clé publique d'Alice à partir d'un BBS (tableau d'affichage électronique). A l'aide de cette clé, vous cryptez votre lettre pour Alice, puis lui envoyez via l'e–mail du BBS.

Malheureusement, à votre insu à tous les deux, un autre utilisateur prénommé Charlie s'est infiltré dans le BBS et a généré sa propre clé publique en y associant l'ID utilisateur d'Alice. En cachette, il remplace la vraie clé publique d'Alice par sa clé erronée. Vous utilisez involontairement la fausse clé de Charlie au lieu de la clé publique d'Alice. Cette fausse clé étant associée à l'ID utilisateur d'Alice, vous ne remarquez rien d'anormal. Charlie peut, à présent, déchiffrer le message rédigé à l'attention d'Alice puisqu'il détient la clé privée

correspondante. Il peut même crypter à nouveau le message déchiffré à l'aide de la vraie clé publique d'Alice et lui renvoyer, de manière à ce qu'aucune infraction ne soit suspectée. Il peut également signer à la place d'Alice avec cette clé privée puisque les signatures d'Alice seront toutes vérifiées via la fausse clé.

Le seul moyen d'éviter un problème de ce type consiste à empêcher quiconque de falsifier des clés publiques. Si Alice vous envoie directement sa clé publique, vous êtes à l'abri de toute mésaventure. Cette opération peut toutefois être difficile à réaliser si Alice se situe à des milliers de kilomètres de vous ou si vous n'arrivez pas à la joindre.

Vous pourriez vous procurer la clé publique d'Alice auprès d'un ami commun, David, qui est sûr de détenir une copie correcte de cette clé. David peut signer la clé publique d'Alice afin de garantir son authenticité. Il peut créer cette signature à l'aide de sa propre clé privée.

Il en résulterait un certificat de clé publique signé, prouvant que la clé d'Alice n'a pas été falsifiée. Pour ce faire, vous devez être certain d'être en possession d'une copie correcte de la clé publique de David afin de vérifier sa signature. Autre solution : David pourrait également fournir à Alice une copie signée de votre clé publique, servant ainsi de « correspondant » entre Alice et vous.

Ce certificat de clé publique signé destiné à Alice pourrait être téléchargé par elle ou par David sur le BBS, d'où vous pourriez ensuite vous-même le télécharger. Vous vérifieriez alors cette signature via la clé publique de David afin de vous assurer qu'il s'agit réellement de la clé publique d'Alice. Aucun imposteur ne peut vous tromper en vous communiquant sa fausse clé comme étant celle d'Alice puisque personne d'autre ne peut falsifier les signatures de David.

Quelqu'un ayant la confiance de nombreuses personnes pourrait remplir les fonctions de « correspondant » d'utilisateurs en fournissant des signatures pour leurs certificats de clés publiques. Cette personne aurait le statut d'« Autorité de certification ». Tout certificat de clé publique comportant la signature de cette Autorité serait fiable et considéré comme appartenant véritablement à la personne censée en être le détenteur. Seule une copie correcte de la clé publique de l'Autorité de certification serait nécessaire aux utilisateurs souhaitant participer, afin de pouvoir vérifier les signatures de l'Autorité. Dans certains cas, l'Autorité de certification peut également remplir la fonction de serveur de clés, permettant ainsi aux utilisateurs d'un réseau de rechercher des clés publiques par son intermédiaire. Toutefois, rien ne justifie la nécessité qu'un tel serveur certifie des clés.

Une Autorité de certification centralisée de confiance est particulièrement adaptée aux grandes sociétés impersonnelles ou aux institutions gouvernementales. Certaines institutions instaurent des hiérarchies d'Autorités de certification.

Dans les milieux moins centralisés, il est probablement plus judicieux que chaque utilisateur agisse en tant que correspondant fiable auprès de ses amis plutôt que de recourir à une Autorité de certification de clé centralisée.

L'un des atouts majeurs de PGP est de fonctionner aussi bien dans un milieu centralisé à l'aide d'une Autorité de certification que dans un milieu décentralisé où les personnes s'échangent leurs clés personnelles.

Cette lutte laborieuse contre la falsification des clés publiques constitue le seul problème difficile à résoudre dans les applications de clés publiques. C'est le « talon d'Achille » de la cryptographie de clé publique qui est à lui seul à l'origine de nombreuses solutions logicielles complexes.

Utilisez une clé publique uniquement lorsque vous êtes certain qu'elle est correcte, non falsifiée et qu'elle appartient réellement à la personne supposée y être associée. Si vous avez obtenu le certificat de clé publique directement de son détenteur ou s'il porte la signature d'une personne en qui vous avez confiance, par exemple vous ayant auparavant fourni une clé publique correcte, alors toutes les garanties sont réunies. En outre, l'ID utilisateur doit porter le nom complet du détenteur de la clé, pas uniquement son prénom.

Aussi tentant cela soit-il, ne vous fiez *jamais* à une clé publique téléchargée à partir d'un BBS, à moins qu'elle ne soit signée par une personne de confiance. Cette clé non certifiée pourrait avoir été falsifiée par n'importe qui, voire par l'administrateur système du BBS.

Si vous devez signer le certificat de clé publique d'un tiers, assurez-vous qu'il appartient réellement à la personne désignée dans l'ID utilisateur du certificat. En effet, en signant ce certificat, vous vous engagez personnellement sur le fait que la clé appartient réellement à la personne concernée. Quiconque se fiant à vous acceptera cette clé publique parce que votre signature y est apposée.
Il peut être dangereux de croire aux « on-dit » : signez une clé publique uniquement si vous avez appris par vous-même qui la détient réellement. L'idéal consiste à ne la signer qu'après l'avoir obtenue directement de son détenteur.

Il est plus important d'être sûr du détenteur d'une clé lorsque vous la signez que lorsque vous souhaitez simplement l'utiliser pour crypter un message. Des signatures de certification apposées par des correspondants de confiance suffisent pour garantir la validité d'une clé. En revanche, avant de signer une clé, renseignez-vous en personne sur l'identité de son détenteur. Vous pouvez éventuellement téléphoner à cette personne et lui lire l'empreinte digitale de la clé afin d'être sûr que la clé lui appartient réellement. Vérifiez que vous vous adressez bien à la bonne personne.

N'oubliez pas que l'apposition de votre signature sur un certificat de clé publique ne garantit pas l'intégrité de son détenteur mais uniquement celle de la clé (c'est à dire de sa détention). Votre crédibilité n'est pas mise en jeu par le fait de signer la clé publique d'un psychopathe alors que vous êtes absolument certain qu'il en est le détenteur. Des tiers accepteraient cette clé comme lui appartenant parce que vous l'avez signée (en partant du principe qu'ils se fient à vous), mais ils ne feraient pas confiance au détenteur. Se fier à une clé et faire confiance à son détenteur sont deux attitudes différentes.

Conservez à portée de main votre clé publique à laquelle sont associées plusieurs signatures de certification de divers « correspondants » garantissant la validité de votre clé. Il reste à espérer que la plupart des gens se fieront à au moins l'un d'entre eux. Vous pouvez placer votre clé et l'ensemble de ces signatures de certification associées sur plusieurs BBS. Lorsque vous signez une clé publique, renvoyez-la à son détenteur de manière à ce qu'il puisse ajouter votre signature à l'ensemble des références qu'il a réunies pour sa clé publique.

Prenez les précautions nécessaires afin que personne ne puisse falsifier votre trousseau de clés publiques. La vérification d'un certificat de clé publique venant d'être signé doit finalement dépendre de l'intégrité des clés publiques fiables placées sur votre trousseau de clés publiques. Exercez un contrôle physique sur votre trousseau de clés publiques, de préférence à partir de votre ordinateur personnel plutôt qu'à partir d'un système distant exploité en temps partagé, ainsi que vous le feriez pour votre clé privée. De cette manière, vous le protégez contre la falsification, mais pas contre la divulgation. Conservez une copie de sauvegarde fiable de votre trousseau de clés publiques et de votre clé privée sur un support protégé en écriture.

Votre clé publique étant utilisée en tant qu'ultime autorité pour certifier directement ou indirectement toutes les autres clés de votre trousseau, il est fondamental de protéger celle-ci en premier lieu contre la falsification. Vous pouvez conserver une copie de sauvegarde sur une disquette protégée en écriture.

PGP part généralement du principe que vous veillez physiquement à la sécurité de votre système et de vos trousseaux de clés, ainsi qu'à celle de votre copie de PGP. Si un intrus peut falsifier votre disque, il peut théoriquement falsifier le programme et, du même coup, affaiblir les systèmes de sécurité du programme permettant de détecter la falsification de clés.

Une façon quelque peu complexe de protéger l'ensemble de votre trousseau de clés contre de telles tentatives consiste à le signer dans son intégralité à l'aide de votre clé privée. Pour ce faire, constituez un certificat de signature séparée de votre trousseau.

Comment PGP localise-t-il les clés correctes ?

Avant de lire cette section, lisez la précédente intitulée « Comment protéger les clés publiques contre la falsification ? »

PGP localise sur votre trousseau les clés correctement certifiées par des signatures de correspondants en qui vous avez confiance. Il vous suffit d'indiquer à PGP les personnes que vous avez désignées comme correspondants et de certifier leurs clés vous-même à l'aide de la plus fiable de vos clés. PGP peut la sélectionner à cet endroit, validant ainsi automatiquement l'ensemble des autres clés signées par vos correspondants désignés. Naturellement, vous pouvez directement signer davantage de clés.

Il existe deux types de critères très différents utilisés par PGP pour juger de l'utilité d'une clé publique. Ne les confondez pas :

1. La clé appartient–elle réellement à la personne censée en être le détenteur ? En d'autres termes, a-t-elle été certifiée par une signature fiable ?

2. Appartient-elle à une personne suffisamment fiable pour certifier d'autres clés ?

PGP peut calculer la réponse à la première question. Quant à la seconde, vous devez répondre de façon explicite à PGP. Une fois cette seconde réponse donnée, PGP est en mesure de calculer celle de la question 1 pour d'autres clés signées par le correspondant déclaré fiable.

Les clés certifiées par un tel correspondant sont estimées correctes par PGP. Les clés détenues par des correspondants fiables doivent elles-mêmes être certifiées par vous-même ou par d'autres correspondants fiables.

PGP offre également la possibilité d'affecter plusieurs niveaux de fiabilité aux personnes désignées comme correspondants. La confiance que vous avez en un détenteur de clé pour qu'il agisse en tant que correspondant ne reflète pas uniquement l'estime que vous avez pour son intégrité, mais aussi pour sa capacité à comprendre la gestion des clés et à faire preuve de discernement lors de la signature de clés. Vous pouvez désigner une personne comme étant non fiable, à fiabilité marginale ou complète en matière de certification d'autres clés publiques. Ces informations relatives à la fiabilité sont stockées avec la clé sur votre trousseau, sauf si vous indiquez à PGP de copier une clé en dehors de votre trousseau de clés. En effet, vos opinions personnelles sur la fiabilité sont confidentielles.

Lorsque PGP calcule la validité d'une clé publique, il examine le niveau de fiabilité de l'ensemble des signatures de certification associées. Il calcule un résultat pondéré. Par exemple, deux signatures à fiabilité marginale sont jugées aussi dignes de foi qu'une seule signature à fiabilité complète. Le scepticisme du programme est réglable. Par exemple, vous pouvez demander à PGP d'exiger deux signatures à fiabilité complète ou trois signatures à fiabilité marginale pour considérer une clé correcte.

Votre propre clé est « implicitement » correcte selon PGP, aucune signature de correspondant n'étant nécessaire pour prouver sa validité. Pour reconnaître vos clés publiques, PGP recherche les clés privées correspondantes sur la clé privée. PGP est également fondé sur le principe que vous vous accordez une confiance totale pour la certification d'autres clés.

Au fil du temps, vous accumulez des clés appartenant à des personnes que vous souhaitez désigner comme correspondants fiables. Toute autre personne choisira ses propres correspondants fiables et accumulera progressivement un ensemble de signatures de certification qu'il distribuera avec sa clé, en supposant que ces destinataires se fieront à au moins une ou deux de ces signatures. Il en résultera une fiabilité du Web décentralisée, tolérant les pannes pour l'ensemble des clés publiques.

Cette approche de base unique dans son genre contraste vivement avec les systèmes de gestion des clés publiques standard élaborés par le gouvernement et autres institutions monolithiques, comme la messagerie étendue de confidentialité (PEM), et qui reposent sur la centralisation du contrôle et de la confiance obligatoire. Ces systèmes standard sont fondés sur une hiérarchie d'Autorités de certification vous imposant les personnes à qui vous fier. La méthode décentralisée probabiliste du programme permettant de déterminer la légitimité de la clé publique constitue la pièce maîtresse de son architecture de gestion des clés. PGP vous laisse choisir qui bon vous semble, et vous place à la tête de votre propre pyramide de certification privée. PGP s'adresse à ceux pensant ne pas être aussi bien servis que par eux-mêmes.

Le fait que l'accent soit mis ici sur cette approche de base décentralisée ne signifie pas que le fonctionnement de PGP soit moins performant dans un système de gestion des clés publiques plus hiérarchisé et centralisé. Par exemple, des utilisateurs appartenant à de grandes entreprises souhaiteront probablement qu'une seule et même personne signe l'ensemble des clés des employés. PGP appréhende ce scénario centralisé comme un cas particulier de dégénérescence du modèle de fiabilité PGP plus répandu.

Comment protéger les clés privées contre la divulgation ?

Protégez très soigneusement votre clé privée et votre mot de passe complexe. Si votre clé privée est compromise, faites-le savoir rapidement à l'ensemble des parties intéressées avant que quiconque ne l'utilise pour signer en votre nom. Par exemple, quelqu'un pourrait l'utiliser pour signer des certificats de clés publiques erronées, ce qui pourrait être très dommageable, surtout si de nombreuses personnes se fient à votre signature. En outre, la compromission de votre clé privée peut s'étendre aux messages vous étant adressés.

La première mesure à prendre pour protéger votre clé privée consiste à toujours en conserver le contrôle physique. Enregistrez-la sur votre ordinateur personnel, chez vous, ou sur votre ordinateur portable. Si, au bureau, vous travaillez sur un ordinateur sur lequel vous n'exercez pas toujours un contrôle physique, conservez vos trousseaux de clés publiques et privées sur une disquette protégée en écriture et prenez-la avec vous en partant. Il serait peu prudent de laisser votre clé privée sur un ordinateur distant exploité en temps partagé, tel qu'un système UNIX à accès distant. Une personne piratant votre ligne modem pourrait s'emparer de votre mot de passe complexe et se procurer votre clé privée à partir du système distant. Utilisez votre clé privée à partir d'un ordinateur placé sous votre contrôle physique.

Ne stockez pas votre mot de passe complexe sur l'ordinateur comportant votre fichier de clés privées. Il est aussi dangereux de stocker à la fois la clé privée et le mot de passe complexe sur le même ordinateur que de conserver son code bancaire et sa carte bleue dans le même portefeuille. Vous ne souhaitez certainement pas que quelqu'un mette la main sur la disquette comportant à la fois votre mot de passe complexe et votre fichier de clés privées. Le mieux est de mémoriser votre mot de passe complexe sans le stocker où que ce soit. Si vous avez besoin d'écrire votre mot de passe complexe sur une feuille, conservez-la en lieu sûr, plus encore que le fichier de clés privées.

Conservez des copies de sauvegarde de clé privée. N'oubliez pas que vous disposez de l'unique copie de votre clé privée et que si vous l'égarez, l'ensemble des copies de votre clé publique distribuées deviendrait inutile.

L'approche décentralisée et non institutionnalisée prise en charge par PGP pour la gestion des clés publiques présente des avantages, mais elle implique également que vous ne pouvez pas compter sur une seule liste centralisée des clés compromises. Cela complique la tâche consistant à limiter les dommages entraînés par la compromission de votre clé privée. Le plus simple consiste à faire fonctionner le bouche à oreille et à espérer que tout le monde sera tenu au courant.

Dans le pire des cas, à savoir la compromission de votre clé privée et de votre mot de passe complexe (en espérant que vous vous en aperceviez), vous devez émettre un certificat de « révocation de clé ». Ce type de certificat sert à signaler à chacun qu'il doit cesser d'utiliser votre clé publique. Vous pouvez créer un tel certificat à l'aide de PGP via la commande Revoke dans le menu PGPkeys ou en demandant à votre autorité de révocation désignée de le générer à votre place. Envoyez-le ensuite à un serveur de certificats, de manière à ce que chacun en prenne connaissance. Les logiciels PGP installent ce certificat de révocation de clé sur les trousseaux clés publiques et empêchent automatiquement l'utilisation accidentelle de votre clé. Vous devez générer une nouvelle paire de clés publiques / privées, puis publier la nouvelle clé publique. Vous pouvez envoyer un seul fichier contenant à la fois votre nouvelle clé publique et le certificat de révocation de clé relatif à votre ancienne clé.

En cas de perte de votre clé privée

En règle générale, lorsque vous souhaitez révoquer votre propre clé privée, vous pouvez utiliser la commande Révoquer du menu PGPkeys afin d'émettre un certificat de révocation, signé avec votre clé privée personnelle.

Mais que faire si votre clé privée est perdue ou endommagée ? Il vous est alors impossible de la révoquer vous-même, car vous avez besoin de cette clé privée que vous venez de perdre. Si votre clé ne dispose d'aucune autorité de révocation désignée, c'est-à-dire d'une personne définie dans PGP comme autorisée à révoquer cette clé en votre nom, vous devez alors demander à chaque utilisateur ayant signé votre clé de retirer sa certification. Ainsi, toute personne tentant d'utiliser votre clé, car elle fait confiance à l'un de vos correspondants, saura qu'elle ne peut pas considérer votre clé publique comme fiable.

Pour plus d'informations sur les autorités de révocation désignées, reportez-vous au *Guide de l'utilisateur PGP*.

Attention aux remèdes de charlatans

Lors de l'évaluation d'un logiciel cryptographique, la question de sa fiabilité se pose toujours. Même si vous pouvez vérifier personnellement le code source, vous ne possédez peut-être pas l'expérience nécessaire pour juger de sa sécurité. Et même si vous étiez un cryptographe expérimenté, certains points faibles des algorithmes pourraient encore vous échapper.

Lorsque j'étais encore étudiant, au début des années soixante-dix, j'ai conçu un système de cryptage que j'estimais particulièrement astucieux. Une simple série de nombres pseudo-aléatoires était ajoutée au texte en clair afin de générer le texte chiffré. Selon toute apparence, ce procédé empêchait une analyse fréquentielle du texte chiffré et s'avérait inviolable, même pour les services de renseignement gouvernementaux disposant de ressources inépuisables. J'étais si fier de mon invention.

Des années plus tard, j'ai découvert ce même système décrit dans plusieurs introductions à la cryptographie et dans divers comptes rendus de séminaires. Formidable ! D'autres cryptographes avaient élaboré le même procédé. Hélas, il était présenté comme un simple exercice d'application aux techniques élémentaires de cryptanalyse et le jeu consistait à casser son code. C'en était fini de mon idée brillante.

De cette expérience humiliante, j'ai appris combien il était facile de se donner l'illusion de la sécurité lors de l'élaboration d'un algorithme de cryptage. La plupart des personnes ne réalisent pas les efforts nécessaires à la conception d'un algorithme de cryptage soumis aux attaques prolongées et déterminées de la part d'un opposant ingénieux. De nombreux ingénieurs informatiques ont développé des systèmes de cryptage plus ou moins naïfs (souvent pratiquement identiques) qui ont parfois été incorporés à des logiciels de cryptage et commercialisés, de manière lucrative, à des utilisateurs peu méfiants.

Cela revient à vendre des ceintures de sécurité automobiles qui semblent parfaites, mais qui ne se verrouillent pas même lors d'un test de collision à basse vitesse. Se fier à leur fiabilité peut s'avérer pire que de ne pas mettre sa ceinture. Tant qu'un accident n'est pas arrivé, personne ne peut douter de leur fiabilité. Un logiciel cryptographique vulnérable peut vous amener à mettre involontairement des informations sensibles en péril, alors que vous auriez su comment les protéger si vous n'aviez pas disposé d'un tel outil. De plus, il est même possible que vous ne découvriez jamais que vos données ont été exposées.

Certains logiciels du commerce ont parfois recours à la norme de cryptage de données fédérale (DES), un algorithme conventionnel assez performant, recommandé par le gouvernement pour un usage commercial (et non pour les renseignements classifiés, ce qui peut paraître plutôt bizarre). DES peut utiliser divers « modes de fonctionnement », certains meilleurs que d'autres. Le gouvernement recommande expressément d'éviter le mode le plus élémentaire et le plus vulnérable pour les messages, c'est-à-dire le mode ECB (dictionnaire de code électronique). En revanche, il conseille vivement les modes CFB (renvoi de chiffrement) et CBC (chaînage de blocs de chiffrement) qui sont plus évolués et plus performants face aux attaques.

Malheureusement, la plupart des modules de cryptage du commerce que j'ai pu examiner utilisent le mode ECB. Au cours de discussions avec les auteurs de certaines de ces implémentations, ils m'ont avoué n'avoir jamais entendu parler des modes CBC et CFB et à ignorer tout des points faibles du mode ECB. Le simple fait que leurs connaissances en cryptographie soient insuffisantes pour être au courant de ces concepts élémentaires n'est pas très rassurant. En outre, leurs clés DES sont souvent conçues d'une manière inappropriée et peu sûre. Mais, plus grave encore, ces mêmes modules logiciels incluent parfois un second algorithme de cryptage plus rapide pouvant être utilisé au lieu

du DES qui est considéré comme plus lent. La plupart du temps, l'auteur de ce module est persuadé que son algorithme propriétaire est aussi sécurisé que l'algorithme DES. Cependant, après quelques questions, je découvre généralement qu'il s'agit en fait d'une variante du procédé brillant que j'avais inventé alors que j'étais étudiant. Ou bien, il refusera peut-être de me révéler le secret de son algorithme, tout en m'assurant de son ingéniosité et de sa fiabilité. Il est sûrement sincère, mais comment le croire sans jeter un coup d'œil au code ?

En toute impartialité, je dois souligner que ces produits aussi peu performants sont souvent élaborés par des entreprises non spécialisées dans les techniques de cryptographie.

Cependant, même les excellents logiciels, qui utilisent l'algorithme DES selon le mode de fonctionnement approprié, présentent également des problèmes. La norme de cryptage DES emploie une clé 56 bits qui, selon les standards actuels, est trop petite et peut désormais facilement être forcée par des recherches exhaustives sur des calculateurs particulièrement rapides. En effet, la norme DES a atteint les limites de sa durée de vie utile, et il en est de même des logiciels basés sur cette norme.

Il existe une entreprise, appelée AccessData (http://www.accessdata.com) qui vend un module à prix modéré permettant de casser certains procédés de cryptage intégrés, tels que ceux utilisés par les applications WordPerfect, Lotus 1-2-3, Microsoft Excel, Symphony, Quattro Pro, Paradox, Microsoft Word et PKZIP. Non seulement, ce module permet de deviner les mots de passe, mais il autorise également une véritable analyse de cryptographie. Certaines personnes s'en servent lorsqu'ils ont oublié le mot de passe de leurs fichiers. Les fonctionnaires chargés de l'application de la loi l'utilisent également pour consulter les fichiers saisis. Après avoir discuté avec Eric Thompson, son auteur, j'ai appris qu'il ne fallait pas plus d'une fraction de seconde à son logiciel pour violer un code, mais qu'il lui avait ajouté une boucle de temporisation afin de ralentir son exécution et donner ainsi l'illusion à l'utilisateur d'une difficulté à résoudre.

Dans le domaine de la téléphonie sécurisée, le choix proposé est plutôt désolant. Le principal produit concurrent est le STU-III (unité téléphonique sécurisée), commercialisé par Motorola et AT&T pour une somme comprise entre 2 000 et 3 000 dollars et utilisé par le gouvernement des Etats-Unis pour ses applications classifiées. Son algorithme de cryptographie est assez complexe, mais une autorisation spéciale du gouvernement est requise pour faire l'acquisition de cette version évoluée. Il existe également, dans le commerce, une version du STU-III qui a été édulcorée à la demande de la NSA, ainsi qu'une version vouée à l'export qui a été rendue encore plus vulnérable. Ensuite, vous pouvez également acquérir Surity 3600 d'AT&T pour la modique somme de 1 200 dollars. Ce produit utilise pour le cryptage la fameuse puce Clipper du gouvernement américain, avec dépôts de clés pour faciliter les écoutes télé-

phoniques. Enfin, vous pouvez bien sûr commander dans les catalogues, soi-disant spécialisés dans les accessoires d'espionnage, des brouilleurs de voix analogiques (non numériques), qui ne sont ni plus ni moins que des gadgets inutiles pour ce qui est de la cryptographie, mais qui sont commercialisés comme produits de communications « sécurisés » à des utilisateurs crédules.

D'une certaine façon, l'éthique dans le domaine de la cryptographie est la même que dans l'industrie pharmaceutique. L'intégrité est une règle cruciale. Il est difficile de distinguer des ampoules de pénicilline de bonne ou de mauvaise qualité. Il est facile d'évaluer un tableur, mais comment savoir si un module de cryptographie est vulnérable ? Rien ne différencie un texte chiffré généré par un algorithme de cryptage défaillant d'un texte chiffré créé par un algorithme performant. Le commerce propose beaucoup de remèdes de charlatan et de médicaments miracle. Mais contrairement aux camelots de l'ancien temps, ces concepteurs logiciels ne savent généralement pas que leur portion n'est que de la poudre de perlimpinpin. Il s'agit sans aucun doute d'ingénieurs informatiques remarquables, mais ils n'ont sûrement jamais lu aucun des ouvrages académiques traitant de la cryptographie. Pourtant, ils restent persuadés qu'ils sont capables de développer un logiciel de cryptage performant. Et pourquoi pas ? A première vue, cela paraît plutôt intuitif. Et leur logiciel semble fonctionner correctement.

Toute personne croyant avoir conçu un procédé de cryptage inviolable est soit un génie hors du commun, soit un grand naïf totalement inexpérimenté. Hélas, j'ai eu souvent affaire à des apprentis cryptographes qui souhaitaient apporter des « améliorations » à PGP en ajoutant des algorithmes de cryptage de leur cru.

Je me souviens d'une conversation avec Brian Snow, un cryptographe éminent de la NSA. Il me déclara qu'il ne pourrait jamais se fier à un algorithme de cryptage, élaboré par quelqu'un qui n'avait pas d'abord gagné ses galons en cassant du code. Cela semblait tomber sous le sens. J'observai alors que pratiquement personne dans le monde commercial de la cryptographie ne répondait à ce critère. « Oui », me répondit-il avec un sourire plein d'assurance, « Et, c'est ce qui rend notre travail à la NSA si facile ». J'en eus froid dans le dos. Je ne possédais pas non plus toutes les compétences requises.

Le gouvernement a également colporté des boniments. Après la deuxième guerre mondiale, les Etats-Unis ont vendu à des gouvernements du tiers-monde des équipements allemands de chiffrement utilisant le code Enigma. Mais, bien sûr, il omirent de préciser que les alliés avaient déjà cassé ce code pendant la guerre, un fait qui demeura classé défense pendant de nombreuses années. Aujourd'hui encore, de nombreux systèmes UNIX, de par le monde, utilisent la méthode de chiffrement Enigma pour le cryptage des

fichiers, en partie car le gouvernement a créé de nombreux obstacles légaux contre l'implémentation de meilleurs algorithmes. En 1977, l'état a même été jusqu'à tenter d'empêcher la publication initiale de l'algorithme RSA et, pendant de longues années, il a littéralement étouffé tout effort commercial pour développer, à l'attention du grand public, des téléphones réellement sécurisés.

La tâche principale de l'agence de sécurité nationale du gouvernement des Etats-Unis consiste à rassembler des renseignements, essentiellement par des écoutes clandestines des communications privées de la population (reportez-vous à l'ouvrage de James Bamford, intitulé *The Puzzle Palace*). La NSA a accumulé des compétences et des ressources considérables dans l'art du piratage de codes. Lorsque la population est dans l'impossibilité de se protéger au moyen d'un système cryptographique efficace, le travail de la NSA s'en trouve ainsi facilité. De plus, l'agence de sécurité nationale du gouvernement des Etats-Unis est également chargée d'approuver et de recommander les algorithmes de cryptage. Certaines critiques font valoir qu'il y a conflit d'intérêt. Autant demander au renard de garder le poulailler ! Dans les années quatre-vingts, la NSA a préconisé l'utilisation d'un algorithme de cryptage qui a avait été créé par ses employés (le programme d'approbation COMSEC), tout en refusant de dévoiler ses rouages sous le prétexte qu'il était classé défense. L'agence souhaitait simplement que tout le monde l'adopte les yeux fermés. Néanmoins, tous les cryptographes vous diront qu'un algorithme correctement conçu n'a pas besoin d'être classé défense pour rester sécurisé. Seules les clés doivent être protégées. Et puis, comment être parfaitement sûr qu'un algorithme classé défense par la NSA est réellement sécurisé ? Si personne ne peut vérifier leur algorithme, cela serait vraiment un jeu d'enfant pour la NSA d'élaborer un code de cryptage qu'ils seraient les seuls à pouvoir casser.

Trois facteurs déterminants sont à l'origine de la qualité médiocre des logiciels de cryptographie commercialisés aux Etats-Unis.

- Le premier réside dans le manque de compétences quasiment généralisé des concepteurs de logiciels de cryptage du commerce (bien que cela soit en train de changer depuis la publication de PGP). Tous les ingénieurs informatiques ont tendance à se prendre pour des cryptographes, ce qui a conduit à une prolifération de logiciels de cryptographie d'un niveau désastreux.

- Le deuxième facteur est dû à la volonté délibérée et systématique de la NSA d'éliminer toute technologie de cryptage valable, par des intimidations juridiques et des pressions économiques. Une partie de ces pressions a été exercée par des contrôles sévères sur l'exportation des logiciels de cryptage dont l'effet immédiat, en raison des lois économiques du marketing, a été d'anéantir la production nationale.

- Le troisième principe à la base de cette méthode d'élimination a consisté à n'accorder des brevets logiciels pour tous les algorithmes de cryptage de clés publiques qu'à une seule et unique entreprise, créant ainsi un goulet d'étranglement afin d'empêcher toute propagation de cette technologie (quoique ce cartel se soit disloqué à l'automne 1995).

Le résultat direct de ces efforts est qu'avant la publication de PGP, il n'existait, aux Etats-Unis, pratiquement aucun logiciel de cryptage polyvalent hautement sécurisé.

Aujourd'hui, je ne suis pas aussi certain de la sécurité de PGP que je ne l'étais jadis lors de mes exploits universitaires. Dans le cas contraire, cela serait vraiment un mauvais signe. Mais, je ne pense pas que PGP présente des défaillances évidentes (bien que je sois à peu près sûr qu'il contienne des bogues). J'ai sélectionné les meilleurs algorithmes dans les publications universitaires traitant de la cryptologie et non destinées à la défense. Pour la plupart, ces algorithmes ont fait l'objet individuellement d'un examen minutieux de la part de mes homologues. Je connais dans le monde de nombreux cryptographes de renom et j'ai discuté avec certain d'entre eux des algorithmes et des protocoles utilisés dans PGP. Ce produit a fait l'objet de recherches exhaustives et sa conception a pris de nombreuses années. Et, le plus important, je ne travaille pas pour la NSA. Toutefois, je ne vous demande pas de me croire sur parole lorsque je vous parle de l'intégrité de PGP, car son code source est disponible afin de faciliter son évaluation.

Il existe enfin une dernière preuve de mon engagement à garantir la qualité de PGP. Depuis les premiers balbutiements de PGP et sa distribution gratuite en 1991, j'ai fait l'objet, pendant trois ans, d'une enquête par les services de douane américains en raison de la diffusion à l'étranger de PGP, avec le risque de poursuites criminelles et de plusieurs années d'emprisonnement. D'ailleurs, auparavant aucun logiciel de cryptographie n'avait jamais autant dérangé le gouvernement (c'est bien PGP qui déclenche toutes ces foudres). Est-ce que cela ne vous en dit pas plus sur la force de PGP ? Toute ma réputation repose sur l'intégrité cryptographique de mes produits. Je ne renierai pas mon engagement à défendre votre droit à la confidentialité pour lequel j'ai risqué ma liberté. Je ne suis pas prêt à apposer mon nom sur un produit qui pourrait comporter un passage secret.

Vulnérabilités

« Si tous les ordinateurs du monde (260 millions) travaillaient ensemble, il leur faudrait tout de même, en moyenne, 12 millions de fois l'âge de l'univers pour casser un seul message crypté par PGP ».

--William Crowell, Directeur adjoint, Agence de sécurité nationale du gouvernement des Etats-Unis, 20 mars 1997.

Aucun système de sécurité de données n'est impénétrable. PGP peut être mis en échec de diverses manières. Dans tout système de sécurité de données, vous devez d'abord vous poser la question si les informations que vous tentez de protéger présentent aux yeux des pirates informatiques une valeur plus importante que le coût de l'attaque elle-même. Cette stratégie devrait vous amener à vous prémunir contre les attaques les moins coûteuses et à ne pas vous tracasser pour les plus onéreuses.

Il est possible que le débat qui va suivre vous paraisse exagérément paranoïaque, mais une telle attitude est parfaitement appropriée lorsque le sujet de la vulnérabilité est abordé.

Sécurité du mot de passe complexe et de la clé privée

L'attaque la plus simple dont vous pouvez faire l'objet peut probablement survenir si vous notez quelque part le mot de passe complexe de votre clé privée. Si quelqu'un arrive à l'obtenir et accède également au fichier de votre clé privée, il pourra alors lire vos messages et effectuer des signatures en votre nom.

Voici quelques recommandations qui vous aideront à protéger votre mot de passe complexe :

1. N'utilisez pas de mots de passe complexes évidents, pouvant facilement être devinés, tels que les noms de vos enfants ou de votre conjoint.

2. Ajoutez à votre mot de passe complexe des espaces, ainsi qu'une combinaison de chiffres et de lettres. Si votre mot de passe complexe est constitué d'un seul mot, il pourra facilement être trouvé par une recherche informatique de tous les mots du dictionnaire. C'est la raison pour laquelle un mot de passe complexe est préférable à un simple mot de passe. Toutefois, un pirate sophistiqué peut parcourir à l'aide de son ordinateur un recueil de citations célèbres afin de deviner votre mot de passe complexe.

3. Faites preuve d'imagination. Utilisez un mot de passe complexe dont vous vous souviendrez facilement, quoique difficile à deviner. Vous pouvez, par exemple, inventer de toutes pièces une phrase absurde ou recourir à une citation littéraire tirée d'un ouvrage d'un auteur obscur.

Falsification de clé publique

Le risque principal de vulnérabilité réside dans la falsification des clés publiques. Ce point faible du système de cryptographie de clé publique est d'une importance cruciale, en partie, car la plupart des novices ne reconnaissent pas immédiatement cette contrefaçon.

En deux mots, lorsque vous utilisez la clé publique de quelqu'un d'autre, assurez-vous qu'elle n'a pas été falsifiée. Vous ne devez vous fier à une clé publique provenant d'un tiers uniquement si vous l'avez obtenue directement de son détenteur ou si elle a été signée par une personne à qui vous faites confiance. Prenez les précautions nécessaires afin que personne ne puisse falsifier votre trousseau de clés publiques. Gardez un œil sur vos trousseaux de clés publiques et privées. Il est préférable de les stocker sur votre ordinateur personnel, plutôt que sur un système partagé distant. Conservez une copie de sauvegarde de vos deux trousseaux de clés.

Suppression de fichiers incomplète

Une des autres menaces pesant sur la sécurité est due au système de suppression des fichiers de la plupart des systèmes d'exploitation. Lorsque vous cryptez un fichier, puis supprimez le texte en clair d'origine, en réalité le système d'exploitation n'efface pas physiquement les données. Il désigne simplement ces blocs disque comme supprimés, autorisant ainsi leur réutilisation ultérieure. Cela revient un peu à jeter des dossiers confidentiels dans la corbeille de recyclage, au lieu d'utiliser le broyeur à documents. Les blocs disque contiennent encore les informations sensibles que vous souhaitiez effacer et seront probablement écrasés par de nouvelles données à un moment ou un autre. Si un pirate informatique lit ces blocs disque effacés immédiatement après leur libération, il pourra alors récupérer votre texte non crypté.

En fait, cette récupération de données résiduelles peut également survenir accidentellement, par exemple, si votre disque ou certains fichiers étaient involontairement effacés ou altérés. Dans un tel cas, il est possible de lancer un programme de réparation afin de tenter de récupérer les fichiers endommagés. Cependant, il arrive alors souvent que des fichiers effacés ressuscitent. Vos fichiers confidentiels que vous croyiez éliminés à tout jamais peuvent ainsi réapparaître, puis être consultés par la personne intervenant sur votre disque. De plus, lors de la création de votre message d'origine à l'aide d'un traitement ou d'un éditeur de texte, cette application génère automatiquement une multitude de copies temporaires de votre texte sur le disque. A la fermeture de votre fichier, ces copies temporaires sont supprimées, mais ces fragments sensibles peuvent demeurer quelque part sur votre disque.

La seule manière d'empêcher la réapparition du texte en clair est de provoquer d'une façon ou d'une autre son écrasement. A moins d'être sûr et certain que tous les blocs disque effacés seront rapidement réutilisés, vous devez prendre des mesures concrètes afin d'écraser le texte en clair, ainsi que tout fragment pouvant avoir été abandonné par votre traitement de texte sur votre disque. Pour effacer toute trace de votre texte confidentiel, utilisez les fonctionnalités d'effacement sécurisé et d'effacement de l'espace libre de PGP.

Virus et chevaux de Troie

Une autre attaque pourrait être occasionnée par un virus informatique hostile qui infecterait PGP ou votre système d'exploitation. Ce virus éventuel serait spécialement conçu pour s'emparer de votre mot de passe complexe, de votre clé privée ou de vos messages cryptés et pour enregistrer clandestinement ces informations volées sur un fichier, transmis ultérieurement via le réseau au détenteur du virus. Il pourrait également altérer le comportement de PGP afin que les signatures ne soient pas correctement vérifiées. Ces attaques sont moins onéreuses que des agressions par cryptanalyse.

La protection contre ce type d'attaque relève du domaine général de la défense contre les infections virales. Il existe dans le commerce des produits antivirus assez performants et il convient de respecter certaines précautions afin de réduire considérablement le risque de propagation d'un virus. Une description exhaustive des mesures antivirales dépasse le cadre de notre présentation. PGP n'est pas protégé contre les virus, car votre ordinateur personnel est supposé fonctionner dans un environnement sûr. Si un tel virus venait à naître, il faut espérer que la nouvelle finirait par se répandre.

Une attaque similaire consiste à créer une imitation astucieuse de PGP, présentant un comportement pratiquement identique à l'original, mais ne fonctionnant pas comme prévu. Par exemple, il est possible d'altérer délibérément l'application afin que les signatures ne soient pas vérifiées correctement, autorisant ainsi la validation de faux certificats de clés. Pour un pirate informatique, il est facile de créer un tel *cheval de Troie,* car le code source de PGP est accessible à tous. Il est donc à la portée de tout informaticien de modifier ce code source, puis d'engendrer un zombie lobotomisé de PGP qui paraît authentique, mais qui suit les ordres de son maître satanique. Ce cheval de Troie pourrait ensuite être diffusé à grande échelle, sous la fausse allégation d'être d'une origine légitime. N'est-ce pas insidieux ?

Cela vaut peut-être la peine de se procurer une copie directement auprès de Network Associates, Inc.

Les signatures numériques peuvent également vous permettre de déceler des signes de falsification éventuels. Il vous suffit alors d'utiliser une autre version fiable de PGP afin de vérifier la signature sur une version suspecte. Cependant, cette méthode ne sera d'aucune utilité si votre système d'exploitation est infecté ou si votre original de l'exécutable pgp.exe a été altéré intentionnellement de façon à compromettre sa capacité à contrôler les signatures. Ce test suppose que vous possédez une copie fiable de la clé publique utilisée pour vérifier la signature sur l'exécutable de PGP.

Fichiers d'échange ou mémoire virtuelle

A l'origine, PGP a été développé pour MS-DOS, un système d'exploitation archaïque selon les standards actuels. Lors de son portage sur des systèmes d'exploitation plus évolués, tels que Microsoft Windows et le Mac OS, un nouveau point faible a émergé. Cette vulnérabilité découle du fait que ces systèmes d'exploitation sophistiqués recourent à une technique appelée la *mémoire virtuelle*.

La mémoire virtuelle vous permet d'exécuter des applications volumineuses qui exigent davantage de mémoire que l'espace disponible sur les circuits intégrés à semi-conducteur de votre ordinateur. Ce procédé est pratique car les logiciels sont de plus en plus gourmands en mémoire depuis que les interfaces graphiques sont devenues la norme et que les utilisateurs ont pris l'habitude d'exécuter simultanément plusieurs applications volumineuses. En règle générale, le système d'exploitation utilise le disque dur pour le stockage des portions de logiciel temporairement non utilisées. Cela signifie que le système d'exploitation peut, à votre insu, écrire sur le disque des informations que vous croyiez conservées uniquement dans la mémoire vive, telles que des clés, des mots de passe complexes et des textes en clair décryptés. PGP ne conserve pas ces données sensibles en mémoire plus longtemps que nécessaire, mais le risque que le système d'exploitation inscrive ces informations sur le disque dur n'est pas exclu.

Ces données sont enregistrées dans une zone de mémoire auxiliaire du disque, connue sous le nom de *fichier d'échange*. Dès que nécessaire, ces informations peuvent être récupérées pour lecture à partir du fichier d'échange, afin de ne stocker dans la mémoire physique qu'une portion de votre application ou de vos données. L'ensemble de cette activité est transparente pour l'utilisateur qui perçoit uniquement les sonorités caractéristiques d'un disque en cours de traitement. Microsoft Windows permute les segments de mémoire, appelés *pages*, à l'aide de l'algorithme de remplacement de page LRU (Least Recently Used). Autrement dit, les pages pour lesquelles l'accès est le moins récent seront les premières à être permutées sur le disque. Selon cette approche, il est probable que le risque de basculer des données confidentielles sur le disque est plutôt réduit, car PGP ne les conserve pas longtemps en mémoire. Toutefois, il est impossible d'apporter une garantie formelle.

En outre, toute personne pouvant accéder physiquement à votre ordinateur peut consulter ce fichier d'échange. Si ce problème vous inquiète, vous pouvez y remédier en vous procurant un logiciel spécifique permettant d'écraser votre fichier d'échange. Une autre solution consiste également à désactiver la mémoire virtuelle. Microsoft Windows et Mac OS possèdent cette fonctionnalité. Toutefois, si vous désactivez la mémoire virtuelle il est possible que vous ayez besoin d'installer des barrettes de mémoire supplémentaires, afin de pouvoir stocker l'ensemble de vos informations sur la mémoire vive.

Violation de la sécurité physique

Une violation de la sécurité peut autoriser un individu à obtenir physiquement vos textes en clair ou les impressions de vos messages. Un adversaire déterminé ne reculera ni devant le cambriolage, la fouille de vos ordures, des enquêtes ou des saisies au-delà du raisonnable, la corruption, le chantage, ni même l'infiltration de votre personnel. Certaines de ces attaques ne paraissent pas si invraisemblables lorsqu'il s'agit d'infiltrer des organisations politiques de masse qui dépendent de nombreux volontaires.

Ne vous laissez pas aller à un sentiment de sécurité trompeur pour la seule raison que vous possédez un outil cryptographique. Ces techniques protègent vos données uniquement lorsqu'elles sont cryptées. Une fuite au niveau de la sécurité peut toujours exposer vos données en clair ou, même, vos informations écrites ou parlées.

Ces attaques sont moins onéreuses que des agressions par cryptanalyse de PGP.

Attaques Tempest

Certains adversaires, particulièrement bien équipés, ont eu recours à la détection à distance des signaux électromagnétiques émis par votre ordinateur. Ce piratage coûteux en termes de technologie et de main-d'œuvre demeure tout de même moins onéreux qu'une attaque par cryptanalyse. Dans ce type de scénario, une camionnette équipée de manière appropriée se gare à proximité de vos bureaux, puis intercepte vos séquences de touches, ainsi que les messages affichés sur l'écran vidéo de votre ordinateur. Tous vos mots de passe, messages, etc. sont ainsi mis en péril. Il est possible de contrecarrer ce type d'attaque par un blindage approprié de votre matériel informatique et de votre câblage réseau afin d'éliminer toute émission de signaux. Cette technologie de blindage électronique, connue sous l'appellation « Tempest », est utilisée par certaines agences gouvernementales et par une partie de l'industrie militaire. Vous pouvez vous procurer ce type de blindage auprès de certains revendeurs de matériel informatique.

Protection contre les horodatages erronés

Un des points vulnérables de PGP quelque peu ignoré consiste pour des utilisateurs malhonnêtes à falsifier les horodatages de leurs certificats et signatures de leur clé publique. Vous pouvez ne pas prendre connaissance de cette section si vous n'êtes pas un utilisateur expérimenté de PGP ou si vous n'êtes pas parfaitement au fait des protocoles de clés publiques.

Rien ne peut empêcher un utilisateur indélicat de modifier le réglage de la date et de l'heure de son horloge système et de générer des certificats et des signatures de clé publique qui paraîtront avoir été créés à un autre moment. Il peut ainsi faire croire que sa signature a été apposée ou que sa paire de clés publique / privée a été créée avant ou après la date réelle. Cet acte peut présenter pour lui certains avantages légaux ou financiers s'il souhaite, par exemple, se ménager une porte de sortie afin de pouvoir répudier une signature.

A mon avis, ce problème de falsification des horodatages des signatures numériques existe déjà pour les signatures manuscrites. N'importe quelle date peut être ajoutée à une signature manuscrite d'un contrat et personne ne semble s'en inquiéter outre mesure. Et même, dans certains cas, une date « incorrecte » sur une signature manuscrite peut ne pas être considérée comme une pratique frauduleuse. Un horodatage peut attester de la date réelle de la signature d'un document ou de la date à laquelle le signataire souhaite que sa signature soit effective.

Dans des situations où il est primordial de pouvoir s'assurer qu'une signature comporte une date correcte et non falsifiée, il suffit de faire appel à un notaire pour certifier et dater la signature. Une méthode analogue peut être appliquée aux signatures numériques. Dans ce cas, il sera demandé à un tiers en qui l'on a toute confiance de contresigner un certificat de signature et d'y apposer un horodatage fiable. Inutile de mettre en place des protocoles excessivement compliqués. Les attestations de signature ont toujours été reconnues comme une manière légitime d'établir la date exacte de la signature d'un document.

Une autorité de certification digne de confiance ou un notaire pourrait créer des signatures certifiées conformes, avec un horodatage authentifié. Ce système ne nécessiterait pas obligatoirement l'intervention d'une administration centralisée. Un correspondant fiable ou une tierce partie désintéressée pourrait même jouer ce rôle, de la même manière que les notaires de nos provinces le font. Lorsqu'un notaire contresigne la signature d'autres personnes, il crée ainsi un certificat de signature d'un autre certificat de signature. Pour les signatures numériques, sa tâche serait pratiquement identique à celle qu'il remplit déjà pour attester des signatures manuscrites. Il lui suffirait ensuite

d'entrer le certificat de la signature (séparé du document signé) dans un registre notarié spécifique. Toute personne pourrait avoir accès à ce registre. La signature du notaire comporterait alors un horodatage certifié conforme qui, du point de vue de la crédibilité et au sens légal le plus strict, serait plus fiable que l'horodatage de la signature d'origine.

Dans son article, paru en 1983 dans IEEE Computer, Denning a déjà traité ce sujet de manière approfondie. Dans des versions ultérieures de PGP, des fonctionnalités facilitant l'attestation des signatures par notaire, avec des horodatage certifiés conformes, pourraient être ajoutées.

Exposition sur des systèmes multi-utilisateurs

A l'origine, PGP a été conçu pour un PC mono-utilisateur, avec contrôle physique direct. Si vous utilisez PGP à votre domicile sur votre ordinateur personnel, vos fichiers cryptés ne risquent pratiquement rien, à moins que quelqu'un ne s'introduise dans votre maison, dérobe votre ordinateur, puis vous persuade de lui indiquer votre mot de passe complexe (ou que celui-ci soit suffisamment simple à deviner).

PGP n'est pas conçu pour protéger vos données sous forme non-cryptées lorsqu'elles sont situées sur un système exposé. De plus, rien ne peut empêcher un intrus d'employer des méthodes sophistiquées pour lire votre clé privée lorsque vous l'utilisez. Vous devez donc tenir compte de ces risques sur les systèmes multi-utilisateurs et adapter vos attentes et votre comportement en conséquence. Dans votre situation particulière, vous devrez peut-être utiliser PGP uniquement sur un système isolé mono-utilisateur directement sous votre contrôle physique.

Analyse du trafic

Même si le pirate est dans l'incapacité de lire le contenu de vos messages cryptés, il peut déduire certaines informations d'importance à partir de la provenance et de la destination de ces messages, de leur taille et de leur heure d'envoi. Cette pratique ressemble à la consultation frauduleuse de votre facture de téléphone quant à vos appels longue distance, pour en déduire quels sont vos correspondants, à quelles dates vous les contactez et la durée de vos conversations, même si elle ne permet pas de connaître la nature de vos appels. Cette technique est appelée l'analyse du trafic. PGP seul ne vous fournit pas de protection contre ce type d'analyse. Pour résoudre ce problème, il convient d'utiliser des protocoles de communication spécialisés, conçus pour réduire les risques d'analyse du trafic dans votre environnement de communication, en y associant, si possible, une aide cryptographique.

Cryptanalyse

Quoique très onéreuse, une attaque extraordinaire basée sur l'analyse cryptographique pourrait être déployée par un individu disposant d'énormes ressources informatiques, telle une agence gouvernementale. Cet individu serait alors en mesure de casser le cryptage de votre clé publique à l'aide d'une quelconque nouvelle technique mathématique secrète. Toutefois, la défense civile n'a cessé d'attaquer la cryptographie des clés publiques, et ce sans succès depuis 1978.

Le gouvernement américain dispose certainement de méthodes secrètes pour casser les algorithmes de cryptage conventionnels utilisés dans PGP. Il s'agit là du pire cauchemar de tout cryptographe. Il n'existe aucune sécurité absolue garantissant la mise en pratique de la cryptographie.

Il n'en demeure pas moins qu'un certain optimisme se justifie. Les algorithmes de clés publiques, de résumés de messages et le chiffrement par bloc utilisés dans PGP ont été développés par certains des meilleurs cryptographes au monde. Les algorithmes de PGP ont subi des analyses de sécurité et des révisions croisées intensives, menées par certains des meilleurs cryptanalystes ne dépendant pas de l'armée.

Par ailleurs, bien que le chiffrement par bloc utilisé dans PGP comporte quelques faiblesses mineures, PGP compresse le texte d'origine avant le cryptage, ce qui permet d'atténuer sensiblement ces faiblesses. Le travail informatique nécessaire au piratage devient alors bien plus onéreux que la valeur intrinsèque du message.

Si votre situation justifie vos craintes quant à des attaques de ce type, il est alors recommandé de contacter un consultant spécialisé dans la sécurité des données, afin de mettre en place des solutions personnalisées adaptées à vos besoins spécifiques.

En résumé, sans une bonne protection cryptographique de vos communications de données, tout pirate peut pratiquement sans effort intercepter vos messages, parfois même avec une certaine routine, et spécialement s'ils ont été envoyés par modem ou système de messagerie. Si vous utilisez PGP et suivez des mesures de précaution raisonnables, le pirate devra redoubler d'efforts et de moyens pour violer votre intimité.

De plus, si vous vous protégez contre les attaques les plus simples et restez confiant quant à la possibilité d'attaques menées par un pirate déterminé et plein de ressources, PGP vous garantira une sécurité presque parfaite.

Glossaire

A5	Algorithme cryptographique secret utilisé dans les téléphones portables en Europe.
AES (norme de cryptage avancée)	Normes agréées NIST (Agence gouvernementale de normes et de technologie) et généralement utilisées au cours des 20 ou 30 prochaines années.
AKEP (protocole d'échange de clés d'authentification)	Transport de clés basé sur un cryptage symétrique permettant à deux parties d'échanger une clé secrète partagée en toute sécurité contre les adversaires passifs.
Algorithme (cryptage)	Ensemble de règles mathématiques (logiques) utilisées au cours des processus de cryptage et de décryptage.
Algorithme (hachage)	Ensemble de règles mathématiques (logiques) utilisées au cours des processus de création du résumé de message et de la génération de la clé / signature.
Algorithme symétrique	Egalement appelé algorithmes de clé unique, de clé secrète et conventionnel. Les clés de cryptage et de décryptage sont soit identiques, soit calculées l'une à partir de l'autre. Il existe deux sous-catégories : Bloc et Flux.
Anonymat	Dissimulation de l'identification d'une entité d'origine ou de qualité d'auteur inconnue ou non déclarée.
ANSI (Institut national américain de normalisation)	Elabore des normes via divers comités de normalisation accrédités (ASC). Le comité X9 met l'accent sur les normes de sécurité relatives à l'industrie des services financiers.
API (interface de programmation d'application)	Permet de tirer parti des fonctionnalités du logiciel en permettant à des logiciels différents d'interagir.
API SSG (API de services de sécurité génériques)	API offrant une sécurité de haut niveau basée sur l'IETF RFC 1508, qui isole le code d'application orienté session des détails de l'implémentation.

ASN. 1 (notation de syntaxe abstraite n° 1)	Norme ISO / CEI relative aux règles de codage utilisées dans les certificats ANSI X. 509. Il existe deux types de règles : DER (règles de codage explicites) et BER (règles de codage de base).
Attaque « au dictionnaire »	Attaque de force brutale calculée visant à deviner un mot de passe en essayant des combinaisons de mots évidentes et logiques.
Authentification	Permet de prouver l'authenticité par la confirmation de l'identité d'une entité.
Autorisation	Confère à une entité une sanction officielle, ainsi que des droits d'accès ou des compétences juridiques.
Blowfish	Chiffrement symétrique d'un bloc de 64 bits constitué de la création d'une clé et du cryptage des données. Algorithme rapide, simple et compact dans le domaine public écrit par Bruce Schneier.
CA (autorité de certification)	Partie tierce de confiance (PTC) créant des certificats constitués d'affirmations quant à divers attributs et les liant à une entité et / ou une clé publique.
Canal sécurisé	Méthode de transfert des informations d'une entité à une autre, de sorte que la réorganisation, la suppression, l'insertion ou la lecture par un pirate soit impossible (SSL, IPSec ou transmission des informations par chuchotement).
CAPI (API de cryptographie)	API de cryptographie de Microsoft pour les systèmes d'exploitation et applications Windows.
Capstone	Puce cryptographique développée par NSA implémentant la fonctionnalité d'un dépôt de clé du gouvernement américain.
CAST	Chiffrement par bloc de 64 bits utilisant une clé de 64 bits, six boîtes de brouillage avec 8 bits en entrée et 32 bits en sortie. Système développé au Canada par Carlisle Adams et Stafford Tavares.
CBC (chaînage de blocs de chiffrement)	Processus permettant d'obtenir un texte en clair, ayant fait l'objet d'une opération OU exclusif avec le bloc de texte chiffré précédent avant son cryptage et, par conséquent, d'ajouter un mécanisme de renvoi vers un chiffrement par bloc.

CDK (kit de développement cryptographique)

Environnement documenté, comprenant une API pour les parties tierces permettant d'écrire des applications sécurisées à l'aide d'une bibliothèque cryptographique spécifique au fournisseur.

CDSA (architecture commune de sécurité des données)

Intel Architecture Labs (IAL) a développé cette structure pour aborder les problèmes de sécurité des données inhérents à Internet et Intranet à utiliser dans les produits Intel ou autres produits Internet.

CERT (équipe de réponse d'urgence informatique)

Centre d'informations fournissant des conseils en matière de sécurité. Le CERT fournit une assistance technique 24h / 24h pour les incidents impliquant la sécurité d'un réseau ou d'un ordinateur. Il est basé au Software Engineering Institute à l'université Carnegie Mellon de Pittsburgh, PA.

Certificat (numérique)

Document électronique associé à une clé publique par une partie tierce de confiance fournissant la preuve que la clé publique appartient à un détenteur légitime et n'a pas été compromise.

Certificat d'autorisation

Document électronique permettant à un utilisateur de prouver ses droits d'accès ou son identité.

Certificat d'identité

Instruction signée qui lie une clé au nom d'une personne et a pour but de déléguer l'autorité de cette personne vers la clé publique.

Certification

Approbation des informations par une entité fiable.

Certification croisée

Deux ou plusieurs organismes ou autorités de certification partageant le même niveau de confiance.

CFM (mode de renvoi de chiffrement)

Chiffrement par bloc implémenté comme un chiffrement de flot d'auto-synchronisation.

CHAP (protocole d'authentification par échange de nombre aléatoire)

Procédé d'authentification de mots de passes, bidirectionnel et basé sur une session.

Chiffrement de flot

Type de cryptage de clé symétrique où la transformation peut être modifiée pour chaque symbole crypté de texte en clair. Ce cryptage est utilisé pour les ordinateurs avec une mémoire tampon de petite taille.

Chiffrement de substitution	Substitution des caractères du texte en clair avec d'autres caractères pour obtenir un texte chiffré.
Chiffrement de transposition	Le texte en clair reste identique, mais l'ordre des caractères est transposé.
Chiffrement par bloc	Chiffrement symétrique opérant sur des blocs de texte en clair et de texte chiffré comprenant généralement 64 bits.
Clé	Moyen permettant d'obtenir ou d'empêcher l'accès, la possession ou le contrôle, représenté par un nombre important de valeurs.
Clé auto-signée	Clé publique signée par la clé privée correspondante pour preuve de son origine.
Clé de demande de destinataires supplémentaires	Clé spéciale indiquant que tous les messages cryptés vers sa clé de base associée doivent également être cryptés automatiquement vers cette clé. Appelée parfois par sa désignation marketing, clé de décryptage supplémentaire.
Clé de session	Clé secrète (symétrique) utilisée pour le cryptage de chaque ensemble de données sur une base de transaction. Une clé de session différente est utilisée pour chaque session de communication.
Clé privée	Elément tenu « secret » d'une paire de clés asymétriques intégrée, appelé généralement clé de décryptage.
Clé publique	Elément, à la disposition du public, d'une paire de clés asymétriques intégrée, appelé généralement clé de cryptage.
Clé secrète	« Clé privée » dans les algorithmes (asymétriques) de clés publiques ou « clé de session » dans les algorithmes symétriques.
Clés asymétriques	Paire de clés utilisateur distincte, mais intégrée comprenant une clé publique et une clé privée. Chaque clé est unilatérale : si elle est utilisée pour le cryptage des informations, elle ne peut pas l'être pour le décryptage de ces mêmes données.
Confidentialité	Action de conserver le caractère privé et secret d'un élément pour toutes les personnes non autorisées.

Consortium Web	Consortium industriel international fondé en 1994, afin de développer des protocoles communs pour l'évolution du World Wide Web.
Contrôle d'accès	Méthode de restrictions d'accès aux ressources, autorisant l'accès uniquement aux entités disposants des droits correspondants.
Cookie	Cookie HTTP d'état de client persistant : fichier ou jeton, transmis du serveur Web vers le client Web (votre navigateur) utilisé pour vous identifier et pouvant contenir des informations personnelles, telles que l'ID et le mot de passe, l'adresse e-mail, le numéro de carte de crédit, etc.
CRAB	Chiffrement par bloc de 1 024 octets (semblable à RM5) utilisant les techniques d'une fonction de hachage à sens unique, développé par Burt Kaliski et Matt Robshaw aux laboratoires RSA.
Cryptage	Processus permettant de camoufler un message en masquant son contenu.
Cryptanalyse	L'art ou la science de transformer le texte chiffré en texte en clair sans connaissance initiale de la clé utilisée pour le cryptage du texte en clair.
Cryptographie	L'art et la science de créer des messages à caractère privé pouvant être signés, protégés contre toute modification avec non répudiation.
CRYPTOKI	Voir PKCS n°11.
Découpage de clé	Division d'une seule clé entre plusieurs parties, aucune d'entre elles n'ayant la capacité de reconstituer la clé.
Décryptage	Processus de conversion d'un texte chiffré en texte en clair.
Dépôt/reprise de clé	Mécanisme permettant à une partie tierce de récupérer des clés cryptographiques utilisées pour la confidentialité des données, avec comme seul but de récupérer des données cryptées.

DES (norme de cryptage de données)
Chiffrement par bloc de 64 bits, algorithme symétrique également appelé algorithme de cryptage des données (DEA) par l'ANSI et DEA-1 par l'ISO. Ce système est largement répandu depuis plus de 20 ans. Il a été adopté comme norme fédérale pour le traitement de l'information (FIPS 46) en 1976.

DES triple
Configuration de cryptage dans laquelle l'algorithme DES est utilisé trois fois avec trois clés différentes.

Diffie-Hellman
Premier algorithme de clé publique, inventé en 1976, utilisant des logarithmes discrets dans un champ fini.

DMS (Système de messagerie de la défense)
Normes publiées par le ministère de la défense américain pour fournir une infrastructure de messagerie sécurisée et fiable à l'échelle de l'entreprise pour les agences gouvernementales et militaires.

DNSSEC (Groupe de travail de sécurité système de nom de domaines)
Projet proposé par l'IETF spécifiant des améliorations du protocole DNS, afin de protéger le DNS contre des modifications de données non autorisées et contre l'usurpation de l'origine des données. L'intégrité et l'authentification des données sont ainsi ajoutées au DNS via des signatures numériques.

DSA (Algorithme de signature numérique)
Algorithme de signature numérique de clé publique proposé par NIST (l'agence gouvernementale de normes et de technologie) pour l'utilisation dans DSS (standard de signature numérique).

DSS (Standard de signature numérique)
Standard proposé (FIPS) par la NIST pour les signatures numériques à l'aide de DSA.

ECC (Système cryptographique de courbe elliptique)
Méthode unique permettant la création d'algorithmes de clés publiques en fonction des courbes mathématiques sur des champs finis ou via des nombres premiers importants.

Echange de clés
Schéma permettant à plusieurs nœuds de transférer une clé de session secrète sur un canal non sécurisé.

EDI (échange de données électroniques)
Echange direct et normalisé de documents commerciaux entre des ordinateurs (bons de commande, factures, paiements, analyses d'inventaire, etc.) entre votre entreprise et vos fournisseurs et clients.

EES (standard de cryptage à dépôts) Standard proposé par le gouvernement américain pour le cryptage à dépôts des clés privées.

Empreinte digitale Identifiant unique d'une clé obtenu par le hachage de parties spécifiques de données de clés.

Entropie Mesure mathématique des incertitudes ou du caractère aléatoire.

FEAL Chiffrement par bloc à l'aide d'un bloc de 64 bits et d'une clé de 64 bits, conçu par A. Shimizu et S. Miyaguchi de NTT au Japon.

Fiabilité Confiance totale en l'honnêteté, l'intégrité, la justice et / ou la fiabilité d'une personne, d'une entreprise ou de toute autre entité.

Fiabilité directe Etablissement d'une confiance port à port.

Fiabilité du Web Modèle de fiabilité largement répandu et utilisé par PGP pour valider la provenance d'une clé publique lorsque son niveau de fiabilité est cumulé en fonction de la connaissance individuelle des « correspondants ».

Fiabilité hiérarchique Série progressive d'entités répartissant la fiabilité dans une structure organisée, généralement utilisée dans les autorités émettant les certificats ANSI X.509.

Filtre Fonction, ensemble de fonctions ou combinaison de fonctions qui applique un certain nombre de transformations à son ensemble d'entrée, générant un ensemble de sortie contenant uniquement les membres de l'ensemble d'entrée répondant aux critères de transformation. Les membres sélectionnés peuvent ou non être transformés dans l'ensemble de sortie résultant. Par exemple, il peut s'agir d'une fonction de recherche acceptant plusieurs chaînes avec des opérateurs booléens ((comme a ou comme b) mais sans c) et faisant éventuellement apparaître les chaînes trouvées dans les résultats.

Filtre primitif	Fonction qui applique une transformation simple à son ensemble d'entrée, générant un ensemble de sortie contenant uniquement les membres de l'ensemble d'entrée qui répondent aux critères de transformation. Par exemple, il peut s'agir d'une fonction de recherche acceptant une seule chaîne et générant une liste de numéros dans lesquels se trouve cette chaîne.
FIPS (Norme fédérale pour le traitement de l'information)	Norme gouvernementale américaine publiée par la NIST (agence gouvernementale de normes et de technologie).
Fonction de hachage	Fonction de hachage unilatérale générant un résumé de message qui ne peut être converti afin d'obtenir l'original.
GAK (Accès gouvernemental aux clés)	Méthode permettant au gouvernement de déposer la clé privée d'une personne.
Gestion des clés	Procédure de stockage et de distribution sécurisés de clés cryptographiques précises. Processus global de génération et de distribution sécurisées d'une clé cryptographique vers des destinataires autorisés.
Gost	Chiffrement par bloc symétrique de 64 bits utilisant une clé de 256 bits, développé dans l'ancienne Union soviétique.
Hachage à sens unique	Fonction d'une chaîne de variable permettant de créer une valeur de longueur fixe et représentant l'image d'origine, également appelée résumé de message, empreinte digitale ou contrôle d'intégrité du message (MIC).
HMAC	Fonction de hachage à sens unique dépendant d'une clé conçue spécifiquement pour être utilisée avec MAC (Code d'authentification de message) et basée sur l'IETF RFC 2104.
Horodatage	Enregistrement de l'heure de création ou d'existence des informations.
HTTP (Protocole de transfert de documents hypertextuels)	Protocole commun utilisé pour le transfert de documents entre différents serveurs ou d'un serveur vers un client.

IDEA (Norme internationale de cryptage de données)	Chiffrement symétrique de bloc de 64 bits utilisant des clés de 128 bits basées sur une combinaison d'opérations de différents groupes algébriques. Algorithme considéré comme l'un des plus complexes.
IETF (Groupe de travail Internet)	Importante communauté internationale ouverte de concepteurs de réseaux, d'opérateurs, de fournisseurs et de chercheurs concernés par l'évolution de l'architecture Internet et l'utilisation normale d'Internet. Cette communauté est ouverte à toute personne intéressée.
Intégrité	Garantie selon laquelle les données ne sont pas modifiées (par des utilisateurs non autorisés) lors du stockage ou du transfert.
Intégrité des données	Méthode garantissant que les informations n'ont pas été modifiées par des moyens illicites ou inconnus.
IPSec	Schéma de cryptage de couche TCP / IP en cours d'étude dans l'IETF (groupe de travail Internet).
ISA/KMP (Association de sécurité sur Internet/Protocole de gestion de clés) Protocol)	Définit les procédures d'authentification d'une paire de communication, de création et de gestion des associations de sécurité, de techniques de génération de clés et de réduction des risques de violation de la sécurité, par exemple, refus de service et reproduction des attaques.
ISO (Organisation internationale de normalisation)	Responsable d'un nombre important de normes, telles que le modèle OSI (interconnexion des systèmes ouverts) et les relations internationales avec l'ANSI quant à X.509.
Kerberos	Protocole d'authentification d'une partie tierce de confiance développé par MIT.
LDAP (Protocole d'accès aux petits clients)	Protocole simple prenant en charge les opérations d'accès et de recherche sur des répertoires contenant des informations telles que des noms, numéros de téléphone et adresses sur d'autres systèmes incompatibles via Internet.
Livre Orange	Livre du centre d'homologation de sécurité intitulé Department of Defense Trusted Computer Systems Evaluation Criteria (critères d'évaluation des systèmes informatiques fiables du ministère de la défense) et définissant les besoins en matière de sécurité.

Logarithme discret	Problème mathématique sous-jacent utilisé dans / par les algorithmes asymétriques, tels que Diffie-Hellman et la courbe elliptique. Il s'agit du problème inverse de l'exponentiation modulaire, qui est une fonction à sens unique.
Longueur de clé	Nombre de bits correspondant à la taille de la clé. Plus la clé est longue, plus elle est complexe.
LRC (Liste de révocation des certificats)	Liste en ligne et à jour des certificats délivrés précédemment qui ne sont plus valides.
MAA (Algorithme d'authentification de message)	Norme ISO permettant un hachage de 32 bits. Cette norme a été conçue pour les ordinateurs centraux IBM.
MAC (Code d'authentification de message)	Fonction de hachage à sens unique dépendant d'une clé et nécessitant l'utilisation de la clé identique pour vérifier le hachage.
MIC (contrôle d'intégrité du message)	Défini à l'origine dans PEM (messagerie étendue de confidentialité) pour l'authentification via RM2 ou RM5. Micalg (calcul de l'intégrité du message) est utilisé dans des implémentations MIME sécurisées.
MIME (extensions de messagerie Internet multi-usages)	Ensemble disponible de spécifications offrant la possibilité d'interchanger du texte dans des langues comprenant des jeux de caractères différents et des e-mails multimédia au sein de systèmes informatiques différents utilisant des normes de messagerie Internet.
MMB (Bloc modulaire en multiplication)	Joan Damen a développé cet algorithme symétrique de la taille d'un bloc / d'une clé de 128 bits, en se basant sur l'algorithme international de cryptage de données (IDEA). Cet algorithme n'est pas utilisé en raison de sa sensibilité à la cryptanalyse linéaire.
Monnaie électronique	Argent électronique stocké et transféré via plusieurs protocoles complexes.
MOSS (Service de sécurité des objets MIME)	Défini dans la demande de commentaire RFC 1848, ce service facilite les services de cryptage et de signature pour MIME, y compris la gestion des clés en fonction de techniques asymétriques (rarement utilisé).

Mot de passe	Séquence de caractères ou mot soumis par un sujet à un système à des fins d'authentification, de validation ou de vérification.
Mot de passe complexe	Mot de passe facile à retenir permettant d'améliorer la sécurité par rapport à un mot de passe simple. Le broyage d'une clé permet de la convertir en clé aléatoire.
MSP (Protocole de sécurité des messages)	Equivalent militaire de PEM, protocole de niveau application compatible X. 400 pour la sécurisation des e-mail, développé par NSA à la fin de 1980.
MTI	Protocole d'accord de clé à une passe développé par Matsumoto, Takashima et Imai, fournissant une authentification de clés mutuelle sans confirmation de clé ou authentification d'entité.
NAT (Traducteur d'adresses réseau)	RFC 1631, routeur connectant deux réseaux : le premier, interne, reçoit des adresses privées ou obsolètes devant être converties en adresses légales avant le transfert de paquets vers l'autre réseau (externe).
NIST (Agence gouvernementale de normes et de technologie)	Département du ministère du commerce américain publiant des normes de compatibilité et d'interopérabilité, appelées FIPS.
Nombre aléatoire	Aspect important de nombreux systèmes de cryptographie et élément nécessaire à la génération d'une(de) clé(s) unique(s) ne pouvant être découverte(s) par un adversaire. Généralement, les nombres réellement aléatoires sont dérivés de sources analogiques et impliquent l'utilisation d'un matériel spécifique.
Nombre pseudo-aléatoire	Nombre résultant de l'application d'algorithmes de rangement à une adresse calculée à des entrées dérivées de l'environnement informatique, par exemple, coordonnées de la souris. Voir Nombre aléatoire.
Non répudiation	Vise à empêcher la répudiation des engagements ou actions précédent(e)s.
Oakley	L'« échange de clés de sessions Oakley » fournit un échange de clés de sessions Diffie-Hellman mixte à utiliser dans une structure ISA / KMP. Oakley fournit la propriété importante de « Secret absolu de la transmission ».

Ouverture de session simple	Connexion unique fournissant un accès à toutes les ressources du réseau.
PAP (Protocole d'authentification par mot de passe)	Protocole d'authentification permettant aux paires PPP de s'authentifier. Ce protocole ne permet pas d'éviter des accès non autorisés, mais identifie seulement le terminal distant.
Pare-feu	Combinaison matérielle et logicielle permettant de protéger le périmètre du réseau public / privé contre des attaques spécifiques et ce, afin de garantir un certain degré de sécurité.
PCT (Technologie de communication privée)	Protocole développé par Microsoft et Visa pour sécuriser les communications sur Internet.
PEM (Messagerie étendue de confidentialité)	Protocole permettant de sécuriser les messageries Internet, (RFC 1421-1424) comprenant des services de cryptage, d'authentification, d'intégrité des messages et de gestion des clés. PEM utilise les certificats ANSI X. 509.
PGP/MIME	Norme IETF (RFC 2015) offrant confidentialité et authentification à l'aide des types de contenu de sécurité MIME (extensions de messagerie Internet multi-usages) décrits dans la demande de commentaire RFC1847, actuellement disponible dans les versions PGP 5.0 et ultérieures.
PKCS (Normes de cryptographie des clés publiques)	Ensemble de normes de facto pour la cryptographie de clés publiques développé conjointement avec un groupement informel d'entreprises (Apple, DEC, Lotus, Microsoft, MIT, RSA et Sun) comprenant des normes d'implémentation spécifiques aux algorithmes spécifiques et indépendantes des algorithmes. Spécifications définissant la syntaxe du message et d'autres protocoles contrôlés par RSA Data Security Inc.
PKI (Infrastructure de clé publique)	Système de certification largement disponible et accessible permettant, avec un niveau de fiabilité plus ou moins élevé, d'obtenir la clé publique d'une entité et de vous assurer qu'elle n'a pas été révoquée.

Pretty Good Privacy (PGP) Application et protocole (RFC 1991) pour la sécurisation du cryptage des e-mail et des fichiers, développés par Phil R. Zimmermann. Publié initialement comme logiciel gratuit, le code source a toujours été à la disposition du public. PGP utilise divers algorithmes, tels que IDEA, RSA, DSA, RM5, SHA-1 pour le cryptage, l'authentification, l'intégrité des messages et la gestion des clés. PGP est basé sur le modèle « Fiabilité du Web » et a été développé à l'échelle mondiale.

PTC (partie tierce de confiance) Partie responsable dans laquelle tous les participants impliqués conviennent à l'avance de fournir un service ou une fonction, telle que la certification, en associant une clé publique à une entité, un horodatage ou un dépôt de clé.

RADIUS (Service d'utilisateurs d'authentification distante) Protocole IETF (développé par Livingston, Enterprise) relatif à la sécurité distribuée protégeant les accès distants aux réseaux et aux services qu'ils offrent contre les accès non autorisés. RADIUS est constitué de deux parties : code du serveur d'authentification et protocoles client.

RC2 (chiffrement Rivest 2) Chiffrement symétrique par bloc de 64 bits, de taille de clé variable. Le secret de fabrication est détenu par RSA, SDI.

RC4 (chiffrement Rivest 4) Chiffrement de flot de taille de clé variable. Cet algorithme a appartenu à RSA Data Security, Inc.

RC5 (chiffrement Rivest 5) Chiffrement par bloc avec une diversité d'arguments, de taille de bloc, de taille de clé et de nombre de tours.

REDOC Algorithme de chiffrement par bloc breveté aux Etats-Unis, développé par M. Wood et utilisant une clé de 160 bits et un bloc de 80 bits.

Références Preuve de crédit et de confiance.

Résumé de message Nombre dérivé d'un message. Si un seul caractère du message est modifié, son résumé est différent.

Révocation Reprise de la certification ou de l'autorisation.

RFC (demande de commentaire)

Document IETF, soit des sous-séries RFC FYI (à titre informatif) correspondant à des présentations et à des introductions, soit des sous-séries RFC STD permettant d'identifier et de définir des normes Internet. Chaque demande de commentaire est indexée par un numéro, facilitant sa récupération (www.ietf.org).

RIPE-RM

Algorithme développé pour le projet RIPE de la Communauté Européenne. Cet algorithme a été conçu pour résister à des attaques de cryptanalyse connues et pour produire une valeur de hachage de 128 bits. Variation de RM4.

RM2 (résumé de message 2)

Fonction de hachage à sens unique de 128 bits conçue par Ron Rivest. Cette fonction dépend d'une permutation aléatoire des octets.

RM4 (résumé de message 4)

Fonction de hachage à sens unique de 128 bits conçue par Ron Rivest. Cette fonction utilise un ensemble simple de manipulations de bits avec des opérandes de 32 bits.

RM5 (résumé de message 5)

Version améliorée et plus complexe de RM4. Il s'agit toujours d'une fonction de hachage à sens unique de 128 bits.

ROT-13 (chiffrement de type Rotation)

Chiffrement de substitution simple (César), se déplaçant de 13 emplacements toutes les 26 lettres.

RSA

Diminutif de RSA Data Security, Inc., se rapportant à Ron Rivest, Adi Shamir et Len Adleman ou à l'algorithme qu'ils ont inventé. L'algorithme RSA est utilisé dans la cryptographie de clés publiques et repose sur le fait qu'il est facile de multiplier deux nombres premiers importants, mais difficile de les factoriser à partir du produit.

S/MIME (extension de messagerie Internet multi-usages)

Norme proposée développée par le logiciel Deming et RSA Data Security pour le cryptage et/ou l'authentification des données MIME. S/MIME définit un format pour les données MIME, les algorithmes devant être utilisés pour l'interopérabilité (RSA, RC2, SHA-1) et les questions opérationnelles supplémentaires, telles que les certificats ANSI X.509 et le transfert via Internet.

S/WAN (réseau étendu sécurisé)

Spécifications initiées par RSA Data Security, Inc. relatives à l'implémentation d'IPSec permettant de garantir l'interopérabilité entre le pare-feu et les produits TCP / IP. L'objectif de S / WAN est d'utiliser IPSec pour permettre aux entreprises d'utiliser conjointement le pare-feu avec les produits TCP / IP, afin de construire des réseaux privés virtuels basés sur Internet.

SAFER (routine de cryptage sécurisée et rapide)

Algorithme de cryptage d'une clé de 64 bits de chiffrement par bloc non propriétaire. Cet algorithme n'est pas breveté et ne nécessite aucune licence. Il a été développé par Massey qui a également mis au point IDEA.

Salt

Chaîne aléatoire concaténée avec des mots de passe (ou nombres aléatoires) avant qu'une fonction à sens unique ne lui soit appliquée. Cette concaténation rallonge et obscurcit de manière efficace le mot de passe, rendant le texte chiffré moins sensible à des attaques au dictionnaire.

Schéma Elgamal

Utilisé à la fois pour les signatures numériques et le cryptage en fonction de logarithmes discrets dans un champ fini. Ce schéma peut être utilisé avec la fonction DSA.

SDSI (Infrastructure simple de sécurité distribuée)

Nouvelle proposition PKI de Ronald L. Rivest (MIT) et Butler Lampson (Microsoft). Permet de définir des groupes et des membres, d'établir des listes de contrôle d'accès et des politiques de sécurité. SDSI a été conçu pour insister sur les espaces des noms locaux liés plutôt que sur un espace de noms globaux hiérarchiques.

SEAL (algorithme informatique de cryptage optimisé)

Chiffrement de flot rapide pour des ordinateurs de 32 bits. Ce chiffrement a été conçu par Rogaway et Coppersmith.

Secret absolu de la transmission

Système de cryptographie dans lequel le texte chiffré ne révèle aucune information relative au texte en clair, à l'exception de sa longueur.

Section lexicale

Partie distincte d'un message contenant un type spécifique de données (par exemple, des données signées en clair, des données cryptées et des données relatives à la clé).

SEPP (Protocole de paiement électronique sécurisé)	Spécification ouverte pour la sécurisation des transactions bancaires via Internet. Développée par IBM, Netscape, GTE, Cybercash et MasterCard.
SESAME (Système européen sécurisé pour les applications en environnement multi-distributeur)	Projet de recherche et développement européen améliorant Kerberos en ajoutant des services d'autorisation et d'accès.
SET (Transaction électronique sécurisée)	Permet l'échange sécurisé de numéros de cartes de crédit via Internet.
SHA-1 (algorithme de hachage sûr)	Révision de SHA (1994), développée par NIST, (FIPS 180-1). Lorsque cet algorithme est utilisé avec DSS, il produit un hachage de 160 bits, identique à RM4, qui est très employé et largement implémenté.
Signature aveugle	Capacité à signer un document sans connaissance de son contenu, comme pour un notaire.
Signature numérique	Identification électronique d'une personne ou d'un élément créé à l'aide d'un algorithme de clé publique. Permet de vérifier chez un destinataire l'intégrité des données et l'identité de l'expéditeur.
SKIP (Clé simple pour IP)	Gestion simple des clés pour les protocoles Internet, développée par Sun Microsystems, Inc.
Skipjack	Algorithme de cryptage d'une clé de 80 bits contenu dans la puce Clipper de NSA.
SKMP (Protocole de gestion de clés sécurisée)	Architecture de reprise de clés proposée par IBM utilisant une technique d'encapsulation des clés, afin de fournir la reprise de la clé et du message à un agent de dépôt d'une partie tierce de confiance.
SNAPI (API de réseau sécurisé)	API fonctionnant sur Netscape pour des services de sécurité fournissant des méthodes de protection des ressources contre des utilisateurs non autorisés, de cryptage et d'authentification des communications et de vérification de l'intégrité des données.

SPKI (Infrastructure de clé publique simple)

Projet de norme proposé par l'IETF (par Ellison, Frantz et Thomas), format de certificat de clé publique, signature associée et autres formats, et protocole d'acquisition de clés. Ce projet a été récemment associé à la proposition SDSI de Ron Rivest.

SSH (manuel de sécurité du site)

Manuel sur lequel le groupe de travail de l'IETF travaille depuis 1994 pour concevoir une paire de documents destinée à l'éducation de la communauté Internet en matière de sécurité. Le premier document est un remaniement complet de la demande de commentaire RFC 1244. Il est destiné aux administrateurs systèmes et réseaux, ainsi qu'aux décideurs gestionnaires (cadres moyens).

SSH (shell sécurisé)

Protocole proposé par l'IETF pour sécuriser la couche de transport en fournissant le cryptage, l'authentification cryptographique des hôtes et la protection de l'intégrité.

SSL (Couche socket sécurisée)

Développée par Netscape pour offrir une sécurité et une confidentialité via Internet. Prend en charge l'authentification du client et du serveur et assure la sécurité et l'intégrité du canal de transmission. Fonctionne sur la couche de transport et imite la « bibliothèque des sockets », ce qui lui permet de ne pas dépendre de l'application. Crypte l'intégralité du canal de communication et ne prend pas en charge les signatures numériques au niveau du message.

STT (Technologie de transaction sécurisée)

Protocole de paiement sécurisé développé par Microsoft et Visa en accompagnement du protocole PCT.

STU-III (Unité téléphonique sécurisée)

Téléphone conçu par NSA pour sécuriser la voix et les communications de données à vitesse réduite. Utilisé par le ministère de la défense américain et leurs mandataires.

Système de cryptographie

Système composé d'algorithmes cryptographiques, de tout texte en clair, texte chiffré et de toute clé.

TACACS+ (système de contrôle d'accès au contrôleur d'accès des terminaux)

Protocole fournissant une authentification d'accès à distance, une autorisation ainsi que les services de comptabilisation et de connexion associés. Ce protocole est utilisé par Cisco Systems.

Texte chiffré	Résultat de la manipulation de caractères ou de bits via une substitution, une transposition ou les deux.
Texte en clair	Caractères lisibles par l'homme ou bits lisibles par l'ordinateur.
Texte en clair	Données ou message lisibles par l'homme avant cryptage.
TLS (Sécurité de la couche de transport)	Un avant-projet IETF de la version 1 se fonde sur le protocole SSL version 3 et fournit la confidentialité des communications sur Internet.
TLSP (Protocole de sécurité de la couche de transport)	Projet de norme internationale ISO 10736.
UEPS (Système de paiement électronique universel)	Application de gestion bancaire basée sur une carte à mémoire (carte de débit sécurisée) développée pour l'Afrique du sud où la faiblesse du système téléphonique rend la vérification en ligne impossible.
UIT-T (Union Internationale des télécommunications - Telecoms)	Anciennement CCITT (Comité consultatif international de téléphonie et de télégraphie), organisme mondial de normalisation des technologies de télécommunications.
Valeur spéciale	Ensemble important non répétitif de lettres de clés aléatoires utilisé pour le cryptage, considéré comme le seul schéma de cryptage à utiliser et inventé par Major J. Mauborgne et G. Vernam en 1917.
Validation	Permet de fournir des autorisations pour utiliser ou manipuler des informations ou des ressources.
Vecteur d'initialisation (VI)	Bloc de données arbitraires servant de point de démarrage au chiffrement par bloc utilisant un mode de renvoi de chaînage (voir chaînage de blocs de chiffrement).
Vérification	Permet d'authentifier, de confirmer ou d'apporter des précisions.

VPN (Réseau privé virtuel)	Permet aux réseaux privés d'effectuer une liaison à partir de l'utilisateur final, sur un réseau public (Internet) directement vers la passerelle d'accueil de votre choix, telle que l'intranet de votre entreprise.
WAKE (Cryptage verbal de clés automatique)	Produit un flot de mots de 32 bits, pouvant faire l'objet d'une opération OU exclusif avec un flot de texte en clair pour obtenir un texte chiffré. Ce cryptage a été inventé par David Wheeler.
X. 509	Certificat numérique UIT-T correspondant à un document électronique reconnu au niveau international, permettant de prouver l'identité et l'appartenance de la clé publique au sein d'un réseau de communication. Il comporte le nom de l'émetteur, les informations d'identification de l'utilisateur, la signature numérique de l'émetteur, ainsi que d'autres extensions éventuelles dans la version 3.
X9. 17	Spécification ANSI détaillant la méthode de génération de nombres aléatoires et pseudo-aléatoires.
XOR	Opération OU exclusif. Méthode mathématique permettant de représenter des différences.

Index

A

C

D

E

F

G

I

L

M

N

P

R

S

T

V

Z