Avant-propos

Nombreux sont ceux pour qui la cryptographie a quelque chose de suspect, voire d'inquiétant. Après tout, les techniques de chiffrement sont des secrets militaires et commerciaux depuis des millénaires. Cinéma et littérature utilisent la cryptographie en fonction des besoins du scénario, sans aucun égard pour son fonctionnement véritable. Ceux qui s'y intéressent de plus près sont rapidement confrontés à des algorithmes suffisamment complexes pour décourager quiconque ne dispose pas de connaissances approfondies en mathématiques. Tout ceci contribue à l'ambiance de mystère qui entoure le sujet.

S'il est vrai que les mathématiques sur lesquelles se basent les techniques de cryptographie actuelles sont complexes, les outils cryptographiques sont eux très simples d'emploi dès lors qu'on a une petite idée du type de chiffrement à employer. L'ouvrage que vous tenez dans vos mains vous guidera étape par étape dans le monde de la cryptographie et des signatures numériques ; il vous apprendra à employer les outils qui protègent vos informations confidentielles tout en les transmettant aux personnes voulues.

Ce livre n'a pas l'ambition d'être exhaustif sur le sujet. Il ne vous apprendra pas à calculer manuellement des clés de chiffrement et ne décrit pas non plus dans les moindres détails chacun des algorithmes et chacune des techniques de chiffrement disponibles. En revanche, il vous en apprendra assez sur les principes du chiffrement et de la signature numérique pour que vous fassiez des choix éclairés en fonction des circonstances.

Vous verrez comment intégrer le chiffrement aux logiciels de courrier électronique les plus employés pour échanger des messages électroniques sécurisés avec vos correspondants, comment installer les systèmes de chiffrement Pretty Good Privacy (PGP) et Gnu Privacy Guard (GnuPG ou GPG) sous Windows, Unix, Linux et Mac OS X et comment les utiliser pour sécuriser vos données personnelles.

Le contenu de ce livre

Ce livre n'est pas un traité exhaustif sur la cryptographie, mais il couvre une large gamme de sujets en rapport avec OpenPGP, PGP et GnuPG.

Le **chapitre 1** explique les principes fondamentaux de la cryptographie. Nous y traitons des principaux types de chiffrement employés par OpenPGP, de la différence entre système de chiffrement et code, et du type de chiffrement à employer avec GnuPG.

Le **chapitre 2** expose les principes de fonctionnement d'OpenPGP. Il y est question du réseau de confiance (*Web of Trust*), de clés et de sous-clés, de trousseaux de clés et de serveurs de clés. Vous y trouverez aussi des conseils pour protéger votre clé, la faire signer, la révoquer et la diffuser auprès de tiers.

Le **chapitre 3** explique comment installer PGP Desktop sous Windows et Mac OS X.

Le **chapitre 4** décrit l'installation de GnuPG, à la fois sous Windows et sous les systèmes de type Unix, Linux et Mac OS X.

Le **chapitre 5** montre de quelle manière les clés OpenPGP sont reliées les unes aux autres. Il y est également question de vérification d'identité et de signature de clés. Le réseau de confiance, évoqué au chapitre 2, est ce qui distingue OpenPGP de tous les autres systèmes cryptographiques, et sans doute son élément le plus important. La sécurité ne repose pas sur les logiciels, mais sur leurs utilisateurs. Malheureusement, les utilisateurs sont également les maillons faibles de tout système de sécurité. C'est à quoi le système tente de remédier et vous verrez dans ce chapitre comment signer les clés, et quelles sont les erreurs à éviter.

Le **chapitre 6** traite de la gestion du réseau de confiance à l'aide de PGP Desktop tandis que le **chapitre 7** est consacré à la gestion du réseau de confiance à l'aide de GnuPG.

À RETENIR **Que sont PGP, OpenPGP et GnuPG ?**

PGP est la première implémentation de la norme OpenPGP tandis que GnuPG en est une plus récente et libre de surcroît. Si la phrase qui précède n'a pour vous aucun sens, poursuivez la lecture. Si au contraire, vous savez exactement ce à quoi elle se réfère, vous pouvez envisager de passer directement au chapitre 1.

Dans le **chapitre 8**, vous verrez comment OpenPGP peut s'intégrer à votre courrier électronique et quels sont les problèmes qui peuvent se poser. Il y sera notamment question de PGP/MIME et du stockage de fichiers chiffrés.

Le **chapitre 9** vous montrera alors comment réaliser cette intégration avec PGP Desktop et votre logiciel de courrier électronique sous Windows.

Dans le **chapitre 10**, vous vous familiariserez avec différents plug-ins permettant de faire fonctionner GnuPG avec les logiciels de courrier électronique les plus courants, aussi bien sous Windows et Mac OS X que Linux.

Le **chapitre 11** conclura le livre par des réflexions sur la manière de minimiser les risques en matière de sécurité, sur l'emploi d'OpenPGP au sein d'une équipe et sur l'utilisation de quelques fonctions supplémentaires de GnuPG et de PGP.

Les **annexes A et B** récapitulent respectivement PGP Command Line et les commandes en ligne de GnuPG.

Quels chapitres lire ?

Cet ouvrage traite d'un seul système cryptographique indépendamment de la plate-forme (Windows, Mac OS X, Linux ou Unix) mais qui peut être employé à l'aide de logiciels tout à fait différents.

Deux logiciels mettant en œuvre ce système sont présentés pour différentes plates-formes, et plusieurs aspects de leur utilisation sont abordés. PGP fonctionne sous Windows et Mac OS X, tandis que GnuPG dispose d'une gamme plus large de systèmes supports qui inclut la famile des Linux/Unix.

Vous n'avez besoin de lire que les chapitres concernant le logiciel que vous avez choisi. Si vous hésitez encore, relisez les sections qui précèdent pour vous aider à prendre une décision, ou lisez simplement l'ensemble du livre : il n'est pas si gros, et tôt ou tard, vous vous féliciterez de bien connaître les deux logiciels. Si toutefois vous êtes sûr de préférer l'un des deux logiciels, sachez que les chapitres 3, 6 et 9 et l'annexe A concernent exclusivement PGP tandis que les chapitres 4, 7 et 10 et l'annexe B n'intéresseront que les utilisateurs de GnuPG. Les autres chapitres sont communs aux deux logiciels.

Remerciements

Écrire un livre demande d'être aidé par un grand nombre de personnes. Pour leurs commentaires sur les divers brouillons et versions de *PGP et GPG*, je dois beaucoup aux personnes suivantes : Henry Hertz Hobbit, J. Wren Hunt, Thomas Jones, Srijith Krishnan Nair, David Shaw et Thomas Sjorgeren. Stephan Somogyi de PGP Corporation m'a apporté sa précieuse connaissance de PGP, et ses encouragements en général. Len Sassaman m'a apporté sa précieuse connaissance de OpenPGP et de son histoire, et m'a rappellé à quel point nos doux espoirs ne coïncident pas toujours avec la dure réalité. Je dois à ces gens ce que j'ai fait de bon, tandis que je suis seul fautif de mes erreurs. Il faut aussi porter le crédit de cet ouvrage aux innombrables cryptographes, chercheurs, administrateurs de la sécurité et développeurs système de l'infrastructure mondiale OpenPGP, sans oublier Phil Zimmermann qui le premier a créé PGP. Je n'aurais rien eu à écrire sans eux.

Le débat d'aujourd'hui autour de la confidentialité est plus intense que jamais, et la modeste parution de ce livre ne le clora pas. Alors que David Brin a certainement raison et que la Transparent Society a probablement raison, il semble que la confidentialité soit réservée à certains : les grandes compagnies et les bureaux gouvernementaux en bénéficient, tandis que nous, gens ordinaires, ne sommes pas dans le même cas. Espérons que ce livre vous en offrira la possibilité.