Jean-Philippe Aumasson

La cryptographie déchiffrée

DUNOD

Cette première édition en langue française est la traduction de la seconde édition de l'ouvrage d'origine.

© Dunod, 2024
11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-087211-4

TABLE DES MATIÈRES

Avant-propos

J'ai écrit le livre que j'aurais aimé avoir quand j'ai commencé à apprendre la cryptographie. En 2005, j'étudiais pour un master près de Paris, et je me suis tout de suite inscrit au cours de cryptographie prévu pour le second semestre. Mais à mon grand désespoir, le cours fut annulé, trop peu d'étudiants l'ayant choisi. « La crypto, c'est compliqué », affirmaient les étudiants qui ont préféré suivre en nombre les classes de graphisme et de bases de données.

J'ai depuis souvent entendu cette affirmation. Mais la cryptographie est-elle *vraiment* si compliquée ? Que ce soit pour jouer d'un instrument de musique, maîtriser un langage de programmation, ou mettre en pratique les connaissances de tout domaine suffisamment complexe, il est nécessaire d'apprendre certains concepts de base et notations, mais cela ne nécessite pas un doctorat. Je pense qu'il en va de même pour devenir un cryptographe compétent. Je pense aussi que la cryptographie est perçue comme étant compliquée car les cryptographes ne l'ont pas suffisamment bien enseignée.

Une autre raison qui m'a motivé à écrire ce livre réside dans le fait que la crypto n'est plus seulement une affaire de crypto — elle est désormais un domaine multidisciplinaire. Pour faire quoi que ce soit d'utile et pertinent dans ce domaine, il vous faut comprendre l'environnement dans lequel elle est utilisée : comment les réseaux et systèmes informatiques fonctionnent, les besoins des utilisateurs, ou comment des adversaires peuvent exploiter les faiblesses d'algorithmes et de leurs implémentations. Autrement dit, vous devez être connecté à la réalité.

◆ *L'approche de ce livre*

Le titre initial du volume original était *Crypto for Real*, afin de souligner l'approche pratique, terre à terre, et sans fioriture que je souhaitais suivre. Pour rendre la cryptographie plus abordable sans pour autant trop la simplifier, j'ai choisi de m'appuyer sur des applications du monde réel. Cela se traduit notamment par des exemples de code et de vrais bugs catastrophiques.

Outre un lien clair avec la réalité, les fondements de ce livre sont sa simplicité et sa « modernité ». J'ai privilégié la simplicité dans la forme plutôt que dans le fond : je présente de nombreux concepts non triviaux, mais sans l'intimidant formalisme mathématique. J'essaie plutôt de transmettre les idées fondamentales de la cryptographie, qui sont plus importantes que la mémorisation d'une liste d'équations. Pour assurer la modernité du livre, je couvre de récentes techniques tels que TLS 1.3 et la cryptographie post-quantique. Je ne m'étale pas sur les algorithmes

obsolètes ou peu sûrs tels que DES ou MD5, bien que RC4 fasse exception à la règle, mais seulement pour discuter de ses défauts.

Serious Cryptography (*La Cryptographie déchiffrée*) n'est pas un guide d'utilisation des logiciels de cryptographie ni un recueil de spécifications techniques, lesquels sont aisément disponibles en ligne. L'objectif premier de ce livre est plutôt de vous enthousiasmer, de mettre fin au mythe selon lequel « la crypto, c'est compliqué », et d'enseigner les concepts fondamentaux en cours de route.

◆ *À qui s'adresse ce livre ?*

En écrivant, j'ai souvent imaginé le futur lecteur comme un développeur ayant été exposé à de la cryptographie, mais restant sur sa faim et frustré après avoir survolé de cryptiques ouvrages et articles scientifiques sur le sujet. Les développeurs ont en effet souvent besoin (et envie) de mieux comprendre la cryptographie afin de ne pas commettre de regrettables choix techniques ; j'espère que cet ouvrage les aidera.

Même si vous n'êtes pas développeur ou ingénieur, ne vous inquiétez pas ! Ce livre n'exige pas de connaissance en programmation, et est accessible à quiconque connaît les bases de l'informatique et possède des connaissances mathématiques du niveau secondaire (notions de probabilité et d'arithmétique modulaire, entre autres).

Cet ouvrage peut néanmoins être intimidant et, malgré son accessibilité, demandera un minimum d'attention pour en tirer le meilleur. Pour l'illustrer, j'aime à dresser une analogie entre les livres et l'alpinisme : tel un guide de montagne, l'auteur montre le chemin à suivre, fournit cordes et piolets pour faciliter l'ascension, mais le lecteur doit lui-même parcourir le chemin. Un effort pourra être nécessaire pour saisir certains des concepts de ce livre, mais vous en serez récompensé.

◆ *Comment ce livre est-il organisé ?*

Le livre contient seize chapitres, organisés en quatre parties. Les chapitres sont relativement indépendants les uns des autres, à l'exception du neuvième, qui décrit les bases des trois chapitres qui le suivent. Je vous conseille cependant de commencer par lire les trois premiers chapitres.

Les fondamentaux

- ✓ **Chapitre 1 : Le chiffrement** présente la notion de chiffrement sûr, depuis les simples schémas au crayon à papier jusqu'au solide chiffrement probabiliste.
- ✓ **Chapitre 2 : L'aléa** décrit comment les générateurs de nombres pseudo-aléatoires fonctionnent, quels sont leurs critères de sécurité et comment les utiliser de façon fiable.

- ✓ **Chapitre 3 : La sécurité cryptographique** couvre les notions théoriques et pratiques de sécurité cryptographique, comparant les approches « prouvable » et « probable ».

La cryptographie symétrique

- ✓ **Chapitre 4 : Les *blockciphers*** concerne les cryptosystèmes traitant les messages bloc par bloc, et en particulier le plus connu d'entre eux : l'*Advanced Encryption Standard* (AES).
- ✓ **Chapitre 5 : Les *streamciphers*** présente les cryptosystèmes produisant un flux de bits pseudo-aléatoires, qui sont XORés avec un message pour le (dé) chiffrer.
- ✓ **Chapitre 6 : Les fonctions de hachage** s'intéresse à des algorithmes qui fonctionnent sans clé secrète, et qu'on retrouve dans la plupart des protocoles cryptographiques.
- ✓ **Chapitre 7 : Hacher avec une clé** explique ce qui se passe quand on combine une clé secrète avec le concept de hachage, et comment s'en servir pour authentifier des messages.
- ✓ **Chapitre 8 : Le chiffrement authentifié** présente les algorithmes qui peuvent à la fois chiffrer et authentifier un message, avec comme exemple le standard AES-GCM.

La cryptographie asymétrique

- ✓ **Chapitre 9 : Les problèmes difficiles** décrit les concepts fondamentaux de la cryptographie à clé publique, en se reposant sur des notions d'informatique théorique du domaine de la théorie de la complexité.
- ✓ **Chapitre 10 : RSA** exploite le problème de la factorisation afin de construire des schémas de chiffrement et de signature sûrs, en se reposant sur une simple opération arithmétique.
- ✓ **Chapitre 11 : Diffie–Hellman** étend la cryptographie asymétrique à la notion d'échange de clé, grâce auquel deux parties établissent une valeur secrète commune en échangeant seulement des valeurs non secrètes.
- ✓ **Chapitre 12 : Les courbes elliptiques** fournit une introduction à la cryptographie basée sur les courbes elliptiques, qui offre des avantages notables en termes de performances.

Des applications

- ✓ **Chapitre 13** : **TLS** se concentre sur le protocole *Transport Layer Security* (TLS), sans doute le plus important protocole de sécurité réseau.
- ✓ **Chapitre 14** : **Quantique et post-quantique** présente les concepts de calcul quantique et de cryptographie post-quantique, un des sujets majeurs en cryptographie appliquée dans les années 2020.

- ✓ **Chapitre 15** : **Cryptomonnaies et cryptographie** conclut avec un aperçu des protocoles cryptographiques utilisés dans les applications blockchain ; ce chapitre est « le boss de fin » du livre.

◆ *Sur cette traduction*

Cette traduction de *Serious Cryptography* est publiée près de sept ans après la première édition. Depuis, la cryptographie et ses applications ont évolué. Aujourd'hui, le terme « crypto » évoque souvent les applications blockchain, le Bitcoin et autres cryptomonnaies, plutôt que la cryptographie elle-même. Malgré les avantages sociétaux discutables de ces technologies, leur influence positive indéniable sur l'avancement de la cryptographie ne peut être négligée. C'est pourquoi j'ai ajouté un nouveau chapitre intitulé « Cryptomonnaies et cryptographie », qui traite des techniques cryptographiques fascinantes employées dans les applications de la blockchain, représentant certaines des avancées les plus intéressantes dans le domaine de la cryptographie.

Réalisée en même temps que la mise à jour de *Serious Cryptography* pour sa seconde édition, cette traduction comporte des modifications substantielles par rapport à l'original. Son contenu a été mis à jour suite aux derniers développements en matière de recherche et application de la cryptographie. Parmi les changements significatifs : la discussion du chapitre 2 sur le générateur d'aléa du noyau Linux a été adaptée au nouveau comportement des interfaces */dev/random* et */dev/urandom* ; le chapitre 12 comporte une nouvelle section sur les schémas de signature EdDSA et Ed25519 ; et le chapitre 14 présente les standards de cryptographie post-quantique du NIST sélectionnés en 2022.

J'ai traduit le texte anglais original moi-même, souhaitant que *La Cryptographie déchiffrée* soit plus qu'une simple traduction, et connaissant la difficulté d'un tel exercice, notamment concernant la traduction des termes techniques. J'ai parfois conservé les termes anglais originaux, ma règle étant d'opter pour le terme le plus commun lors de discussions orales entre experts ; par exemple, je parle de *blockciphers* et non de chiffres par bloc. Lorsqu'un terme est traduit, je mentionne entre parenthèses le terme original, afin que les lecteurs puissent facilement rechercher le terme dans la littérature anglophone ; par exemple, je présente les signatures à seuil (*threshold signatures*). J'espère que cet ouvrage offrira aux lecteurs francophones, qu'ils soient étudiants ou professionnels aguerris, une compréhension approfondie des principes fondamentaux de la cryptographie, et qu'il s'avérera être un atout précieux dans leur parcours professionnel.

◆ *Remerciements (de l'édition originale)*

Je tiens à remercier Jan, Annie, ainsi que toute l'équipe de No Starch Press ayant contribué à ce livre, et tout particulièrement Bill pour avoir cru en ce projet dès le départ, et pour son laborieux travail d'édition ayant grandement contribué

à la qualité du texte. Je suis également reconnaissant à Laurel pour son attention à la mise en page.

Concernant la partie technique, un bon nombre d'erreurs et imprécisions ont été évitées grâce aux personnes suivantes : Jon Callas, Bill Cox, Niels Ferguson, Philipp Jovanovic, Samuel Neves, David Reid, Phillip Rogaway, Erik Tews, et les nombreux lecteurs qui ont signalé des fautes dans le texte. Je remercie Matthew Green de m'avoir fait l'honneur d'écrire la préface.

Je remercie de plus Kudelski Security, dont j'étais l'employé pendant l'écriture de ce livre, et qui m'a permis d'y dédier une partie de mon temps de travail. Ma profonde gratitude va enfin à Alexandra et Melina, pour leur soutien et leur patience.

Lausanne, le 17/05/2017 (trois nombres premiers)[1]

◆ *Remerciements (de la traduction)*

Je tiens tout d'abord à remercier les lecteurs de la première édition, en particulier ceux qui m'ont contacté pour me faire part de leurs commentaires et m'aider à améliorer le livre. Je suis reconnaissant envers Dunod, éditeur de l'ouvrage traduit, pour sa confiance et son professionnalisme (merci à Matthieu Daniel et Anne Temps). Merci à André Sintzoff pour sa relecture méticuleuse de l'ouvrage. Il va sans dire, les lacunes de ce livre sont les miennes.

Lausanne, le 28/02/2024

1. Date de l'écriture de la préface dans l'édition originale.

Préface

Si vous avez déjà lu un livre ou deux sur la sécurité informatique, vous aurez sûrement rencontré un jugement récurrent sur le domaine de la cryptographie. « La cryptographie », dit-on, « est le plus fort maillon de la chaîne ». Élogieux, certes, mais quelque peu simpliste. Si la cryptographie était en réalité le composant le plus fiable d'un système, pourquoi investir autant de temps à l'améliorer alors que tant d'autres parties du système pourraient bénéficier de notre attention ?

S'il y a une chose que j'espère que vous retiendrez de cet ouvrage, c'est que cette vision de la cryptographie est idéalisée ; c'est en grande partie un mythe. La cryptographie est solide *en théorie*, mais en pratique elle est aussi fragile que toute autre partie du système. C'est particulièrement vrai quand les implémentations sont développées sans l'expertise, l'expérience, et l'attention adéquate, comme c'est le cas de nombreux systèmes cryptographiques déployés aujourd'hui. Et plus grave encore : lorsque des implémentations cryptographiques ont des problèmes, les conséquences sont souvent remarquablement impressionnantes.

Mais pourquoi s'en inquiéter, et pourquoi ce livre ?

Quand j'ai commencé à travailler dans le domaine de la cryptographie appliquée il y a une vingtaine d'années, l'information disponible pour les développeurs de logiciels était souvent parcellaire et dépassée. Les cryptographes développaient des algorithmes et protocoles, les ingénieurs en cryptographie les implémentaient pour créer des bibliothèques impénétrables et mal documentées destinées principalement à d'autres experts. Il y avait — et il y a toujours — un grand clivage entre ceux qui connaissent et comprennent la cryptographie, et ceux qui l'utilisent (ou l'ignorent, à leurs risques et périls). Il y a peu de livres décents disponibles sur le sujet, et encore moins qui offrent des outils utiles aux professionnels.

Les résultats n'étaient pas beaux à voir. Je parle de problèmes impliquant les termes « CVE » et « Severity: High » et, dans certains cas alarmants, des présentations classées « TOP SECRET ». Vous connaissez peut-être certains des exemples les plus célèbres, ne serait-ce que parce qu'ils ont affecté des systèmes dont vous dépendez. Nombre de ces problèmes sont dus au fait que la cryptographie est subtile et mathématiquement élégante, et que les experts en cryptographie n'ont pas partagé leurs connaissances avec les ingénieurs qui écrivent les logiciels.

Heureusement, cela a commencé à changer et ce livre est un symptôme de ce changement.

Le présent ouvrage, *La Cryptographie déchiffrée*, a été écrit par l'un des plus grands experts en cryptographie appliquée mais il ne s'adresse pas seulement

aux experts. Il ne se limite toutefois pas à un aperçu superficiel du domaine. Au contraire, il offre une discussion approfondie et actualisée de l'ingénierie cryptographique, écrite pour aider les praticiens du domaine à mieux faire. Dans ces pages, vous apprendrez non seulement comment fonctionnent les algorithmes cryptographiques, mais aussi comment les utiliser dans de vrais systèmes.

Le livre commence par une exploration des principales primitives cryptographiques, dont les algorithmes de base tels que les chiffrements par bloc, schémas à clé publique, fonctions de hachage, ou générateurs de nombres aléatoires. Chaque chapitre présente des exemples concrets du fonctionnement des algorithmes, et ce que vous devez ou ne devez *pas* faire. Les derniers chapitres couvrent des sujets plus avancés, comme TLS, ainsi que l'avenir de la cryptographie — ou que faire lorsque des ordinateurs quantiques viendront nous compliquer la vie.

Bien qu'aucun livre ne puisse résoudre tous nos problèmes, un minimum de connaissances peut tout changer. C'est la promesse de cet ouvrage, qui en contient assez pour que la cryptographie réelle et déployée soit à la hauteur des grandes attentes qu'elle suscite chez beaucoup d'entre nous.

Bonne lecture.

Matthew D. Green

Professeur

Information Security Institute

Johns Hopkins University, USA