Sériousse Cryptographie

Préface

Sériousse Cryptographie est une traduction de l'ouvrage **Serious Cryptography**, de Jean-Philippe Aumasson, publié en 2017 par No Starch Press, voir https://nostarch.com/seriouscrypto.

L'extrait ci-dessous est publié sur le site de l'auteur : https://www.aumasson.jp/.

Si vous trouvez des erreurs dans le livre, merci de les reporter à jeanphilippe.aumasson@gmail.com.

v20221015

Préface

J'ai écrit le livre que j'aurais aimé avoir quand j'ai commencé à apprendre la crypto. En 2005, j'étudiais pour un master près de Paris, et je me suis tout de suite inscrit au cours de crypto 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 remplir les classes de graphisme et de bases de données.

J'ai depuis souvent entendu « la crypto c'est compliqué ». Mais la crypto est-elle *si* compliquée ? Que ce soit pour apprendre un instrument, maîtriser un langage de programmation, ou mettre en pratique les connaissances de nombreux domaines fascinants, 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 compliquée car les cryptographes ne l'ont pas suffisamment bien enseignée.

Une autre raison qui m'a motivé à écrire ce livre est 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.

Sériousse Cryptographie 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 de « la cryptographie c'est compliqué », et d'enseigner les concepts fondamentaux en cours de route.

Pour Qui Est 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 and programmation, et est accessible à quiconque connaît les bases de l'informatique et possède des connaissances mathématiques du niveau secondaire (notions de probabilité, 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. J'aime bien cette analogie entre les livres et l'alpinisme : tel un guide de montagne, l'auteur montre le chemin à suivre, vous fournit cordes et piolets pour faciliter l'ascension, mais vous devez vous-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 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 suivants. 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 papier–crayon jusqu'au solide chiffrement probabiliste.
- **Chapitre 2 : L'Aléa** décrit comment les générateurs 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 Crypto Symétrique

- **Chapitre 4 : Les Blockciphers** concerne les cryptosystèmes traitant les messages bloc par bloc, et en particulier le plus connu d'entre eux, le *Advanced Encryption Standard* (AES).
- **Chapitre 5 : Le 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 Crypto Asymétrique

- **Chapitre 9 : Des 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 de 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 partis 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.

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** s'intéresse aux notions de calcul quantique et de cryptographie post-quantique, un des bouleversements majeurs en matière de cryptographie appliquée dans les années 2020.
- **Chapitre 15 : Blockchain** TODO
- **Chapitre 16 : Zero-Knowledge** TODO

Remerciements

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 évités 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 l'avant-propos.

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]

[1] Date de l'écriture de la préface dans l'édition originale. Sa traduction a été réalisée le 28/02/2022, dans un bar bruyant de Lausanne.