Cryptographie par la pratique avec Python et OpenSSL

Cours et applications concrètes

Rémi Boulle
Enseignant à l'IUT de Blagnac

Préface de Stéphane Bortzmeyer

DUNOD

J'adresse mes sincères remerciements à Stéphane Bortzmeyer qui m'a fait l'honneur de préfacer cet ouvrage.

Je remercie aussi vivement Gilles Peskine. Sa relecture rigoureuse et constructive a contribué significativement à la qualité de ce livre.

Gilles Peskine est développeur de systèmes informatiques sécurisés. Normalien et docteur en informatique, il cherche à répondre à la question : comment peut-on être sûr qu'un ordinateur fait bien ce qu'il est censé faire ? Il est mainteneur de la bibliothèque de cryptographie Mbed TLS, utilisée principalement dans les systèmes embarqués, et dont il a notamment redéfini l'interface d'appel des primitives cryptographiques.

Direction et conception graphique de la couverture
Nicolas Wiel – Pierre André Gualino (graphiste)

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-087909-0

Sommaire

Préface

Par Stéphane Bortzmeyer

En 1995, alors que la cryptographie en France était quasiment interdite aux civils, Stéphane Bortzmeyer a publié une tribune dans le journal *Le Monde* appelant à sa libéralisation. C'est un des premiers textes publics sur la question [1]. Ingénieur en réseaux informatiques, il est auteur de plusieurs RFC (documents qui codifient divers aspects de l'Internet) et a publié *Cyberstructure, l'Internet, un espace politique* [2], prix du livre Cyber 2019 catégorie cybersécurité dans le cadre du Forum international de la cybersécurité. Il tient un blog sur l'Internet : `https://www.bortzmeyer.org/`.

Quel est le point commun entre une féministe iranienne qui communique avec des camarades en Allemagne, un lycéen brésilien qui regarde TikTok au lieu de réviser, une banquière suisse qui transfère des fonds et un courtier ivoirien qui regarde les cours du cacao ? Sans en avoir conscience, tous et toutes, dans leur utilisation de l'Internet, utilisent la cryptographie pour se protéger.

Aujourd'hui, alors que beaucoup d'activités humaines ont migré, de gré ou de force (pensons aux services publics qui ne sont souvent accessibles qu'en ligne !), vers l'Internet, les enjeux de la cryptographie sont encore plus importants. Contrairement à ce qu'essaie de faire croire une certaine propagande, le but de la cryptographie n'est pas d'obscurcir ce qui était en clair avant mais au contraire de retrouver la relative vie privée qui existait avant la numérisation. Alors que vous pouviez autrefois prendre le train, acheter un livre, discuter avec des amis, sans donner votre nom, et sans laisser de traces, la numérisation a rendu tout enregistrable et espionnable. La cryptographie est donc le principal outil technique pour limiter ces possibilités d'enregistrement et d'espionnage. À ce titre, elle est une composante indispensable de l'Internet.

Il ne suffit pas qu'un vendeur affirme « ne vous inquiétez pas, c'est crypté » pour être protégé. Les détails comptent. L'utilisation fiable de la cryptographie n'est pas toujours simple. C'est pour cela que le livre de Rémi Boulle est extrêmement utile. Il est nécessaire que des compétences en cryptographie soient plus largement répandues, pour que davantage de personnes puissent participer aux débats politiques impliquant de la cryptographie. Ce livre est

1. `https://www.bortzmeyer.org/crypto.html`
2. `https://cfeditions.com/cyberstructure/`

clair, pédagogique et explique progressivement les concepts, avec des exemples concrets.

Le sujet est riche, et connaître les algorithmes de cryptographie n'est qu'une étape. Il faudra aussi apprendre les limites de la cryptographie qui, comme toute technique, résout des problèmes mais ne fait pas de miracles. Ainsi, la cryptographie ne protège pas contre l'entité avec qui vous communiquez. En termes religieux, « la cryptographie permet de s'assurer qu'on communique bien avec le diable, et que les anges ne peuvent pas écouter, mais elle ne peut pas garantir que Satan est digne de confiance ». Ce rappel est d'autant plus important à une époque où la communication est malheureusement médiée par un petit nombre de grosses entreprises. Faire du HTTPS avec Gmail ne va pas empêcher Google de lire les messages.

La cryptographie, je l'ai dit, doit être utilisée correctement. Ainsi, comme dans l'exemple ci-dessus, il est préférable qu'elle fonctionne de bout en bout, c'est-à-dire que ce qui est chiffré sur votre machine ne soit déchiffré que sur la machine de votre correspondant ou correspondante et pas par un intermédiaire. Le chiffrement de bout en bout n'est pas un détail technique, c'est un facteur très important dans la sécurité.

J'en profite d'ailleurs pour donner un conseil de lecture pour un livre (en anglais) qui parle de cryptographie sous un tout autre angle : « *Concealing for freedom* », de Ksenia Ermoshina et Francesca Musiani, qui traite des aspects sociaux et humains de la sécurité informatique et notamment de la cryptographie (avec des questions du genre « pourquoi les féministes iraniennes utilisent WhatsApp et pas Signal », parce que, comme le note Rémi Boulle, il y a des pays où « le simple fait de vouloir chiffrer une image ou un document fait de vous un suspect »).

Revenons justement au livre de Rémi Boulle. Je recommande aux étudiant·es de le lire, de faire les exercices, de comprendre ce qui se passe. Vous aurez ainsi acquis une meilleure compréhension de ces algorithmes (même si, évidemment, il est déconseillé de les programmer soi-même pour une utilisation réelle : il y a beaucoup de pièges, qu'il n'est pas possible de couvrir dans un livre d'introduction). Mais vous aurez aussi acquis une meilleure idée de ce que la cryptographie permet, et de ce qu'elle ne permet pas.

À l'heure où j'écris, la Commission Européenne essaie toujours de faire passer le règlement CSAM (*Child Sexual Abuse Material*, dit « Chat Control »), qui forcerait les systèmes de messagerie (comme Signal, WhatsApp, Proton et autres) à examiner les messages envoyés. Si la messagerie en question chiffre, cela obligerait à casser le chiffrement pour cet examen. Certains partisans de cette directive prétendent que non, en jouant sur les mots. Mieux connaître la cryptographie aide à déjouer des arguments trompeurs !

Stéphane Bortzmeyer

1

Enjeux et définitions

Le mot « cryptographie » vient du grec ancien kruptos *qui signifie « caché » et de* graphein *qui signifie « écrire ». L'objectif premier est de permettre la communication entre deux entités sans qu'une tierce partie, qui peut voir passer tous les messages et les lire, ne puisse les comprendre.*

1.1 Pourquoi la cryptographie ?

La cryptographie a pour buts principaux d'assurer les points suivants :

- Confidentialité : qui peut lire le contenu des messages ? Il faut s'assurer que les informations ne soient lisibles que par les personnes autorisées. Cela est souvent réalisé grâce au chiffrement, qui transforme les données pour les rendre incompréhensibles sauf à disposer d'une information secrète telle qu'une clé de déchiffrement.
- Intégrité : est-ce que les informations ont été modifiées intentionnellement (le plus souvent à des fins frauduleuses) ou accidentellement ? Il doit être rendu très difficile de modifier le contenu d'un message sans que cela ne soit détecté. Les fonctions de hachage en sont le composant principal.
- Authenticité : est-ce bien la bonne personne qui m'envoie ces données ? On ne doit pas pouvoir émettre des messages en se faisant passer pour quelqu'un d'autre. Ceci peut être réalisé par des signatures numériques (avec, par exemple, des certificats délivrés par des autorités de confiance), des *tokens*, ou des codes d'authentification de message (MAC).
- Non-répudiation : est-ce que l'auteur d'un message ou d'une transaction peut ensuite nier en être à l'origine ? À la manière de la signature d'un chèque, on ne peut pas répudier sa signature. Les signatures numériques sont un outil clé.