Notes de cours de Cryptographie

Yann Miguel

15 janvier 2021

Table des matières

1 Introduction

La cryptographie regroupe trois concepts de base:

1. l'intégrité
2. la confidentialité
3. l'authentification

Si le problème concerne un de ces trois points, alors c'est un problème cryptographique.

L'intégrité, c'est garantir qu'un message n'a subi aucune modification depuis son envoi. Cela est très utile lors de téléchargement, et est primordial pour le commerce électronique.

Il y a deux types de confidentialité, celle des documents sur un support, et celle de communication sur un canal.
La confidentialité utilise un système de chiffrement pour que seul ceux authorisé puissent voir les données.
Le chiffrement de données date de la Rome antique, avec un système de chiffrement basique. on décale chaque lettre de trois position vers la droite. Cette méthode de chiffrement s'appelle le **chiffrement par décalage**.
Il doit donc y avoir un nombre de clé **rédhibitoire**, c'est à dire trop élevé pour toutes les tester une à une.
En juin 2016, le supercalculateur Sunway TaihuLight était le plus puissant calculateur au monde, avec 10^{17} opérations par seconde.
Comme norme de sécurité, l'ANSSI recommande des clés de 128 bits au minimum.

Et, enfin, il y a deux types d'authentification. L'authentification interactive, qui entre en jeu lors d'une communication directe avec un interlocuteur, et la signature électronique, qui consiste à attacher à un message une preuve non-interactive de son origine, ce qui est crucial pour le commercve électronique.

Les principes de Kerckhoff définissent les principes de base à un bon système de chiffrement.

Il y a deux types de chiffrements symétriques:

1. celui par blocs, on découpe le texte en bloc
2. celui par flots

Différences cryptographie symétrique et assymétrique:

- la cryptographie assymétrique crée 2× plus de clés que la symétrique
- la symétrique est 100 à 100× plus rapide que l'assymétrique

D'après Snowden, la NSA ne peux toujours pas casser le PGP, mais cette information peut être fausse maintenant. Le PGP est un système hybride ente la cryptographie symétrique et assymétrique.

La **non-répudiation** est un concept de droit qui empêche de nier un contract. Elle consiste à prouver qu'un message a bien été émis par son expéditeur, ou qu'il a bien été reçu par son destinataire.

2 Cours 1

Une fonction de hachage sert à transformer un message de taille quelconque en un résumé court de taille constante.
Une fonction de hachage cryptographique doit garantir qu'une modification du message de base modifiera le résumé correspondant.

La fonction de hachage cryptographique permet de s'assurer l'intégrité des fichiers téléchargés car il y a très peu de chances que le fichier corrompu ai le même résumé que le fichier voulu.

Le chiffrement de mot de passe est nécessaire dans un système informatique qui demande un mot de passe pour y accéder.
Étant donné qu'on sait faire des collisions pour MD5, ce système de hachage doit être proscrit de nos jours.

La signature numérique d'un document est fabriquée à partir du chiffrage du message avec une clé privée.
Il est essentiel que la fonction de hachage utilisée dans une signature électronique sois résistante à la collision.
La collision est le fait que deux textes différents aient le même résumé. Une fonction de hachage n'ayant pas de résistance à la collision ne peux pas être utilisée en cryptographie.

3 Cours 2

3.1 Cryptographie symétrique par flots

Afin de faire un cryptage symétrique par flot, on peux faire un ou exclusif entre un message formé de n bits et une clé secrète de même taille. Dans ce cas, le déchiffrement sera la même opération que le chiffrement. Il semblerait que ce système fut utilisé par le Kremlin et la Maison Blanche.
Il est important de changer de clé entre chaques messages afin d'éviter les attaques à clairs connus.
Les chiffrements par flots peuvent être implémentés avec une mémoire réduite, et sont très adaptés à des moyens de calculs, de mémoire, et de transmission contraints, tel que les téléphone, ou un usage militaire.

3.1.1 Système RC4

Le système RC4 fut inventé par l'un des inventeurs du RSA, Ronald Rivest. Il est utilisé par le WEP, le WPA, le cryptage proposé par BitTorrent, les pdfs, et est aussi en option dans des systèmes comme SSH et SSL.
Il utilise un chiffrement de type Vernam, c'est à dire un ou exclusif comme expliqué plus haut.

3.1.2 Registres à décalage linéaire (LFSR)

Dans ce type de registre, on obtient la suite pseudo-aléatoire formant les bits de la clé longue à partir d'une relation de récurrence linéaire. Le calcul du bit s_{i+L} s'effectue facilement à partir d'un circuit synchrone muni de L bascules D qui conservent les valeurs des L derniers bits produits.
Cependant, la structure linéaire de ce système le rend peu sûr pour une utilisation cryptographique.

3.2 Cryptographie symétrique par blocs

Dans un chiffrement par blocs, on coupe le texte en blocs, et on chiffre chaque bloc indépendamment. Les blocs font au moins 128 bits.

3.2.1 Bourrage de fichiers

Le bourrage de fichiers consiste à ajouter des octets après le message clair. Le dernier octet du fichier inique le nombre d'octets ajoutés.

3.2.2 Modes opératoires

Il y a différents modes opératoires:

- ECB(Electronic CodeBook): on découpe les blocs et on les chiffre indépendamment, mode très naif.
- CBC(Cypher Bloc Chaining): on choisit un vecteur d'initialisation aléatoire, et on le stocke avec le bloc chiffré. Les blocs suivants utilisent le bloc précédent comme vecteur d'initialisation.

Il existe d'autres modes opératoires, certains évitant le bourrage.

4 Informations importantes

MCC: 0.75*×Examen + 0.25×Projet