

Notes de cours de Cryptographie

Yann Miguel

8 janvier 2021

Table des matières

1	Introduction	2
2	Cours 1	4
3	Informations importantes	5

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 autorisé 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 **réduisant**, c'est à dire trop élevé pour toutes les tester une à une.

En juin 2016, le supercalculateur Sunway TaihuLight était le plus puissant ordinateur 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 commerce 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 asymétrique:

- la cryptographie asymétrique crée $2 \times$ plus de clés que la symétrique
- la symétrique est 100 à $100 \times$ plus rapide que l'asymétrique

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

La **non-répudiation** est un concept de droit qui empêche de nier un contrat. 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 chiffage 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 peut pas être utilisée en cryptographie.

3 Informations importantes

MCC: $0.75 \times \text{Examen} + 0.25 \times \text{Projet}$