Initiation à la Cryptographie

Exploration des Fondements de la Cryptologie, du Chiffrement Simple à la Sécurité Inconditionnelle

January 13, 2025

Awaleh HOUSSEIN

Introduction

- **Cryptologie**: Science du secret, composée de :
  1. **Cryptographie** : Art de rendre un message illisible. Protège les données en garantissant entre autres:

- la **confidentialité** : empêcher leur divulgation à des tiers non autorisés;
- **l'intégrité**: s'assurer qu'elles n'ont pas été modifiées;
- **l'authentification**: vérifier l'identité des utilisateurs et des dispositifs;
- **la non-répudiation**: empêcher de nier des actions, notamment dans le cadre de transactions.

  2. **Cryptanalyse**: Art de "casser" les systèmes de chiffrement. Étudie les failles pour évaluer la sécurité.

Nous allons maintenant nous intéresser à la cryptographie et voir comment la confidentialité est assurée.

Chiffrement et Déchiffrement

Le **chiffrement** est utilisé pour garantir la **confidentialité** en transformant un message clair en un message illisible.

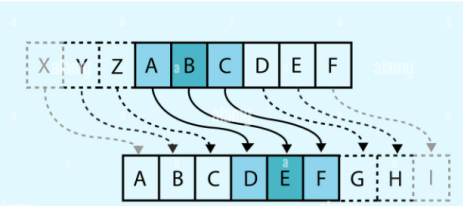
- Le **chiffrement** : $Enc(M, k) = C$ transforme un message M en message chiffré C avec une clé k.
- Le **déchiffrement** : $Dec(C, k) = M$ permet de retrouver le message original à partir de C avec la clé k.

Important

Pour rendre un message illisible, on dit qu'il est **chiffré**, pas *crypté*. ~~Crypter~~ ne signifie rien !

Chiffrement antique: Chiffrement de Césear

Principe : Chaque lettre du message est remplacée par une lettre décalée d'un certain nombre de positions dans l'alphabet. **Exemple (décalage de 3)**[1] :



Exemple pratique :

- Message clair : "ATTAQUEZ"
- Message chiffré : "DWWDTXHC"

Limites :

- Facile à casser par analyse fréquentielle des lettres.

[1] Image source: wikipedia

Chiffrement de Vignère

- Le chiffrement de Vigenère utilise 26 alphabets décalés, améliorant ainsi le chiffrement de César.
- Il utilise une clé pour définir un décalage pour chaque lettre (A=0, B=1, ..., Z=25).

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z

Table: Exemple de chiffrement de Vigenère avec la clé "BACHELIER" [2]

Avantages :

- Chiffrement **polyalphabetique** (plusieurs décalage pour chaque lettre).

Limites :

- Clé courte ou répétitive:
  - vulnérable à l'analyse de Kasiski

[2] Table source: https://www.apprendre-en-ligne.net/crypto/vigenere/index.html

Principes de la cryptographie moderne

Principe de Kerchkoffs

La sécurité d'un chiffrement doit dépendre du secret de la clé, et non de l'algorithme.

Principes de Claude Shanon

Un sytème de chiffrement (cryptosystème) doit apporter les principes suivantes [a] :

- **Confusion** : complexifier la relation entre la clé et le texte chiffré, rendant difficile la déduction de l'un à partir de l'autre.
- **Diffusion** : répartir uniformément l'information du texte en clair dans le texte chiffré, de sorte qu'un changement dans le texte clair affecte largement le texte chiffré.

[a] Claude E. Shannon, Communication Theory of Secrecy Systems

Chiffrement parfait

Définition du secret parfait

Un cryptosystème est qualifié de **secret parfait** si, lorsqu'un texte chiffré c est intercepté, celui-ci ne révèle absolument aucune information sur le texte clair m qui a été chiffré pour générer ce texte. Autrement dit, même en possédant c, il est impossible de déduire quoi que ce soit sur m. Cela peut être exprimé par la condition suivante :

$$\forall m, c, \quad P(m|c) = P(m)$$

Un exemple de chiffrement parfait est le chiffrement de Vernam, présenté dans les slides suivantes.

Chiffrement de Vernam (masque jetable)

- Le masque jetable (en anglais One Time Pad (OTP)) utilise la propriété XOR (OU Exclusif).

$$1 \oplus 1 = 0,\ 1 \oplus 0 = 1,\ 0 \oplus 0 = 0$$

- Masque jetable (OTP) inventé par Vernam en 1917 et amélioré par Mauborne qui a introduit la notion de la clé aléatoire.

Principes d'un OTP

- Clé doit être utilisée une seule fois (d'où le terme jetable)
- La taille de la clé doit être aussi longue que le message.
- Les bits composant la clé, ou masque doivent être choisis aléatoirement .

Fonctionnement de l'algo OTP

Chiffrement et Déchiffrement d'OTP

- Chiffrement:

$$c = Enc(k, m) = k \oplus m$$

- Déchiffrement:

$$m = Dec(k, c) = k \oplus c$$

Exemple:

- Alice souhaite envoyer un message $M = 1001$ à Bob, la clé secrète est $k = 0101$.
- **Chiffrement**: Alice calucle le chiffré $c = M \oplus k = 1001 \oplus 0101 = 1100$.
- **Déchiffrement**: Bob à son tour déchiffre le message chiffré à l'aide la clé k pour retrouver le messsage m.

$$M = c \oplus k = 1100 \oplus 0101 = 1001$$

Avantages et limites du chiffrement de Vernam (OTP)

Avantages:

- Sécurité inconditionnelle: Probabilité discrète uniforme des messages chiffrés.
- Efficacité: XOR est très simple à calculer en informatique.

Inconvénient:

- Clé aussi longue que le message: Problème de stockage, d'accessibilité et de confidentialité des clés.

À retenir

- La cryptologie se divise en **cryptographie** et **cryptanalyse**.
- La **cryptographie** assure la *confidentialité, l'intégrité, l'authentification et la non-répudiation*.
- Le **chiffrement** est utilisé pour garantir la *confidentialité*.
- Deux principes clés pour la cryptographie moderne :
  1. **Principe de Kerchkoffs** : la sécurité d'un cryptosystème repose uniquement sur sa clé secrète.
  2. **Principe de Shannon** : un système de chiffrement doit assurer la **confusion** et la **diffusion**.
- Un cryptosystème est dit *inconditionnellement sûr* si la connaissance du texte chiffré ne révèle aucune information sur le texte clair.
- Exemple de cryptosystème *inconditionnellement sûr* : le chiffrement de Vernam (OTP).