

## 0.1 Références

- Wikipédia
- Le livre "Handbook of Applied Cryptography" de Menezes

# 1 Histoire et contexte

## 1.1 Schéma d'une situation cryptographie

Alice veut envoyer un message  $m$  "en clair" à Bob. Elle doit utiliser un canal non sécurisé. Elle utilise un algorithme de chiffrement  $E$  pour chiffrer son message  $m$  en  $m'$ . Elle envoie  $m'$  à Bob. Souvent une clé  $k$  peut être utilisée. Sur le canal non sécurisé, Eve peut intercepter  $m'$  voire le modifier. Eve peut aussi essayer de retrouver  $m$  à partir de  $m'$ .

### Définition 1.1.

La **cryptographie** est l'étude des techniques mathématiques liées à la sécurité de l'information. Les buts sont:

1. Inaccessibilité de l'information à un tiers.
2. Authentification de l'origine du message.
3. Inaltération du message.

### Définition 1.2.

La **cryptanalyse** est l'étude des techniques mathématiques mettant en défaut les techniques de cryptographie.

**Remarque 1.1.** L'ensemble des techniques de cryptographie et de cryptanalyse est appelé la **cryptologie**.

**Exemple 1.1.** 1. (X - VII siècle avant JC) Scytale (bâton roulé)

2. (V siècle avant JC) Passage de la bible en hébreu
3. (-50 avant JC) César (décalage de 3 dans l'alphabet)

Contextes d'utilisation historique pré-informatique:

- Guerres (communication entre les troupes)

- Association de personnes susceptible d'être menacée
- Diplomatie (négociation)
- Commerce (négociation)
- Infidélité (lettres)

Les canaux de communication:

- Messenger
- Pigeon voyageur
- Journeaux
- Internet
- Télégraphe
- Radio

## **1.2 Techniques cryptographie (avec date)**

- (-200 avant JC) Substitution monoalphabétique (ex: César)  
cassé en 800
- (1585) Vigenère (substitution polyalphabétique)  
cassé en 1863 par Kasiski
- (1919) Enigma (utilisé pour la seconde guerre mondiale par l'armée allemande)  
cassé en 1941 par Alan Turing

## **1.3 Rupture du numérique**

- Explosion de la puissance de calcul
- Automatisation du cryptage et du décryptage
- Nécessité d'échanger des clefs à distance (sur le canal non sécurisé)
- Systèmes plus global (beaucoup de Eve)
- Facilité de dupliquer l'information

utilisations modernes:

- Messages privés (sms, mail, whatsapp, telegram, signal)
- Authentification (mdp, carte bancaire, biométrie)
- Signature électronique (contrat, logiciel)

Futur:

- Développement de l'informatique quantique il y a donc un besoin de nouveaux systèmes cryptographiques "post-quantique"

## 2 Formalisation de la cryptographie

### Définition 2.1.

Un **alphabet** est un ensemble fini de symboles.

### Définition 2.2.

Un **message** dans un alphabet  $A$  est une suite finie à valeurs dans  $A$ .  
noté  $m = m_1 m_2 \cdots m_n$  où  $m_i \in A$  et l'ensemble des messages est noté  $\mathcal{L}(A) = \bigcup_{n \in \mathbb{N}} A^n$ .

### Définition 2.3.

Soient deux messages  $m = m_1 \cdots m_n, m' = m'_1 \cdots m'_p \in \mathcal{L}(A)$   
La concaténation de  $m$  et  $m'$  est définie par  $m'' = m \| m' = m_1 \cdots m_n m'_1 \cdots m'_p$

### Définition 2.4.

Une fonction de chiffrement est une fonction  $E : \mathcal{M} \rightarrow \mathcal{C}$  où  $\mathcal{M}, \mathcal{C} \subset \mathcal{L}(A)$

- $\mathcal{M}$  est l'ensemble des messages pouvant être crypté
- $\mathcal{C}$  est l'ensemble des messages cryptés

### Définition 2.5.

Une fonction de déchiffrement pour  $E$  est une fonction  $D : \mathcal{C} \rightarrow \mathcal{M}$  tel que  $\forall m \in \mathcal{M}, D(E(m)) = m$  i.e.  $D \circ E = Id$

### Proposition 2.1

$E$  est injective

**Démonstration 2.1.**

Soient  $m, m' \in \mathcal{M}$

$$E(m) = E(m') \implies D(E(m)) = D(E(m')) \implies m = m'$$

□

**Proposition 2.2**

$D$  est surjective

**Démonstration 2.2.**

à faire

□

**Définition 2.6.**

Un **cryptosystème** est un quadruplet  $(\mathcal{M}, \mathcal{C}, \mathcal{K}, (E_e, D_d)_{(e,d) \in \mathcal{K}})$  où  $\mathcal{M}, \mathcal{C} \in \mathcal{L}(A)$ ,  $\mathcal{K}$  est un ensemble de paires de ("clef de cryptage", "clef de décryptage").

Pour chaque  $(e, d) \in \mathcal{K}$  on a  $E_e : \mathcal{M} \rightarrow \mathcal{C}$  est une fonction de cryptage ayant  $D_d : \mathcal{C} \rightarrow \mathcal{M}$  pour une fonction de décryptage.

Soit  $A = \{A, \dots, 0\} \simeq \llbracket 0, 25 \rrbracket$

**Exemple 2.1** (César).  $\mathcal{M} = \mathcal{C} = \mathcal{L}(A)$

$$\mathcal{K} = \{(e, d) | e \in \llbracket 0, 25 \rrbracket \text{ et } d = -e\} = \{(e, -e) | e \in \llbracket 0, 25 \rrbracket\}$$

$$D_\alpha = E_\alpha$$

$$\forall m_i \in A, D_\alpha(m_i) = m_i + \alpha \pmod{26}$$

**Exemple 2.2** (Par permutation). Soit  $l$ : longueur des permutations considérées.

$$\mathcal{M} = \mathcal{C} = \bigcup_{n \in \mathbb{N}} A^{nl}$$

$$\mathcal{K} = \{(\sigma, \sigma^{-1}) | \sigma \in \mathfrak{S}_l\}$$

Si  $m = m_1 \cdots m_l$  est de longueur  $l$

$$E_\sigma(m) = m_{\sigma(1)} \cdots m_{\sigma(l)} \text{ et } D_\tau = E_\tau$$

**Exemple 2.3** (Monoalphabétique).  $\mathcal{M} = \mathcal{C} = \mathcal{L}(A)$

$\mathcal{K}$  indexé par  $\text{to}\Delta S(A)$