Chapitre 1 : Introduction à la Cryptographie et Sécurité Parfaite

Cours de Sécurité Informatique - Niveau Universitaire
Partie 1 : Cryptographie à Clé Secrète

12 janvier 2026

Table des matières

1 Introduction

1.1 Objectifs du chapitre

Ce chapitre introduit les concepts fondamentaux de la cryptographie moderne et présente la notion de **sécurité parfaite** (perfect security) telle que formalisée par Claude Shannon en 1949. Nous étudierons :

— Les notions de base : plaintext, ciphertext, clé, chiffrement, déchiffrement

— Les principes de Kerckhoffs et la sécurité moderne

— La définition formelle de la sécurité parfaite

— Le One-Time Pad : seul chiffre prouvé parfaitement sécurisé

— Les limitations fondamentales de la sécurité parfaite

— Les propriétés du XOR et leur importance cryptographique

1.2 Contexte historique

La cryptographie a évolué d'un art empirique à une science mathématique rigoureuse :

— **Antiquité** : Chiffres de substitution (César, Vigenère)

— **1917** : Invention du One-Time Pad par Gilbert Vernam

— **1949** : Shannon formalise la sécurité parfaite dans "Communication Theory of Secrecy Systems"

— **1976** : Diffie-Hellman révolutionne avec la cryptographie à clé publique

— **Aujourd'hui** : Cryptographie basée sur la complexité computationnelle

2 Notions fondamentales

2.1 Définition d'un système cryptographique

Définition

Système de chiffrement (Encryption Scheme)
Un système de chiffrement est un tuple $(\mathcal{M}, \mathcal{K}, \mathcal{C}, \mathsf{Enc}, \mathsf{Dec})$ où :

— $\mathcal{M}$: espace des messages clairs (plaintexts)

— $\mathcal{K}$: espace des clés (key space)

— $\mathcal{C}$: espace des messages chiffrés (ciphertexts)

— $\mathsf{Enc} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$: algorithme de chiffrement

— $\mathsf{Dec} : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$: algorithme de déchiffrement

Propriété de correction : Pour tout $k \in \mathcal{K}$ et $m \in \mathcal{M}$:

$$\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = m$$

2.2 Notations

Nous adoptons les notations suivantes :

— m : message clair (plaintext)

— k : clé (key)

— c : message chiffré (ciphertext)

— $c = \mathsf{Enc}_k(m)$ ou $c = \mathsf{Enc}(k, m)$: chiffrement de m avec la clé k

— $m = \mathsf{Dec}_k(c)$ ou $m = \mathsf{Dec}(k, c)$: déchiffrement de c avec la clé k

— $\{0,1\}^n$: ensemble des chaînes binaires de longueur n

— $\{0,1\}^*$: ensemble des chaînes binaires de longueur arbitraire

— $|x|$: longueur de la chaîne x

— $x \xleftarrow{\$} X$: x tiré uniformément aléatoirement dans X

2.3 Exemple : Chiffre de César

Le chiffre de César est un exemple classique (bien qu'obsolète) de chiffrement par substitution.

Exemple

Chiffre de César

— $\mathcal{M} = \mathcal{C} = \{A, B, \ldots, Z\}^*$: messages en lettres majuscules

— $\mathcal{K} = \{0, 1, \ldots, 25\}$: décalages possibles

— $\mathsf{Enc}_k(m)$: décaler chaque lettre de m de k positions dans l'alphabet

— $\mathsf{Dec}_k(c)$: décaler chaque lettre de c de $-k$ positions (ou $26 - k$)

Exemple concret :

— Message : HELLO

— Clé : $k = 3$

— Chiffrement : KHOOR ($H + 3 = K, E + 3 = H, \ldots$)

— Déchiffrement : HELLO ($K - 3 = H, H - 3 = E, \ldots$)

Faiblesse : Seulement 26 clés possibles $\Rightarrow$ attaque par force brute triviale !

3 Principes de Kerckhoffs

3.1 Énoncé des principes

En 1883, Auguste Kerckhoffs énonce six principes pour la cryptographie militaire. Le plus important est devenu un dogme de la cryptographie moderne :

Théorème

Principe de Kerckhoffs (moderne)
La sécurité d'un système cryptographique ne doit reposer que sur le secret de la clé, jamais sur le secret de l'algorithme.
En d'autres termes : même si l'adversaire connaît parfaitement les algorithmes Enc et Dec, il ne doit pas pouvoir casser le système sans connaître la clé k.

3.2 Justifications

Ce principe se justifie par plusieurs arguments pratiques et théoriques :

1. **Secret difficile à maintenir** : Les algorithmes finissent toujours par fuiter (reverse engineering, traîtres, captures)
2. **Standardisation** : Permet d'utiliser des algorithmes publics, standardisés et largement testés
3. **Analyse de sécurité** : Une communauté mondiale peut analyser et auditer les algorithmes

4. **Renouvellement des clés** : Plus facile de changer une clé compromise qu'un algorithme entier
5. **Principe de Pareto** : Concentrer les efforts de protection sur la gestion des clés

Avertissement

Security through obscurity
La "sécurité par l'obscurité" (cacher l'algorithme) est une mauvaise pratique universellement rejetée en cryptographie moderne. Les algorithmes secrets sont toujours faibles car non audités.

4 Sécurité parfaite (Perfect Security)

4.1 Modèle de l'adversaire

Avant de définir la sécurité, nous devons préciser le modèle d'attaque :

— **Ciphertext-only attack** : L'adversaire observe uniquement $c = \mathsf{Enc}_k(m)$
— **Known-plaintext attack** : L'adversaire connaît des paires (m_i, c_i)
— **Chosen-plaintext attack (CPA)** : L'adversaire peut chiffrer des messages de son choix
— **Chosen-ciphertext attack (CCA)** : L'adversaire peut aussi déchiffrer des ciphertexts

Dans ce chapitre, nous considérons l'attaque la plus faible : **ciphertext-only**.

4.2 Définition de Shannon

Shannon a formalisé la notion intuitive de "sécurité parfaite" : le ciphertext ne révèle **aucune information** sur le plaintext.

Définition

Sécurité Parfaite (Perfect Secrecy)
Un système de chiffrement $(\mathcal{M}, \mathcal{K}, \mathcal{C}, \mathsf{Enc}, \mathsf{Dec})$ a la **sécurité parfaite** si pour tout $m \in \mathcal{M}$ et tout $c \in \mathcal{C}$:

$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

où la probabilité est prise sur le choix uniforme de la clé $K \xleftarrow{\$} \mathcal{K}$ et $C = \mathsf{Enc}_K(M)$.
Interprétation : Observer le ciphertext c ne change pas la probabilité a priori du message m. L'adversaire n'apprend rien !

4.3 Définition équivalente

Une définition équivalente (souvent plus pratique) est :

Proposition 4.1. *Un système a la sécurité parfaite si et seulement si pour tous $m_0, m_1 \in \mathcal{M}$ et $c \in \mathcal{C}$:*

$$\Pr[\mathit{Enc}_K(m_0) = c] = \Pr[\mathit{Enc}_K(m_1) = c]$$

où $K \xleftarrow{\$} \mathcal{K}$.

***Interprétation** : Le ciphertext c est équiprobable quel que soit le message chiffré. Impossibilité de distinguer !*

Démonstration. Par le théorème de Bayes :

$$\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \cdot \Pr[M = m]}{\Pr[C = c]}$$

La sécurité parfaite impose $\Pr[M = m \mid C = c] = \Pr[M = m]$, donc :

$$\Pr[C = c \mid M = m] = \Pr[C = c] \quad \forall m, c$$

Comme $\Pr[C = c \mid M = m] = \Pr[\mathsf{Enc}_K(m) = c]$ (clé uniforme), on obtient l'équivalence. □

5 Le One-Time Pad (OTP)

5.1 Construction

Le **One-Time Pad** (masque jetable), inventé par Gilbert Vernam en 1917, est le seul système prouvé parfaitement sécurisé.

Définition

One-Time Pad (OTP)

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$: messages, clés et ciphertexts de longueur n bits
- Gen : Choisir $k \xleftarrow{\$} \{0,1\}^n$ uniformément aléatoirement
- $\mathsf{Enc}_k(m) = m \oplus k$: XOR bit-à-bit
- $\mathsf{Dec}_k(c) = c \oplus k$: XOR bit-à-bit (identique !)

Propriété de correction :

$$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus 0^n = m$$

5.2 Rappel : Propriétés du XOR

L'opération XOR ($\oplus$) a des propriétés cruciales :

1. **Commutativité** : $a \oplus b = b \oplus a$
2. **Associativité** : $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
3. **Élément neutre** : $a \oplus 0 = a$
4. **Inverse** : $a \oplus a = 0$
5. **Randomisation parfaite** : Si $k \xleftarrow{\$} \{0,1\}^n$, alors $m \oplus k$ est uniforme sur $\{0,1\}^n$, indépendamment de m !

La propriété 5 est **la clé** de la sécurité du OTP.

5.3 Théorème de sécurité

Théorème

Théorème : Le One-Time Pad a la sécurité parfaite
Le OTP défini ci-dessus satisfait la sécurité parfaite au sens de Shannon.

Démonstration. Soit $m_0, m_1 \in \{0,1\}^n$ deux messages arbitraires et $c \in \{0,1\}^n$ un ciphertext arbitraire.

Il existe une unique clé $k_0 = m_0 \oplus c$ telle que $\mathsf{Enc}_{k_0}(m_0) = c$.

De même, il existe une unique clé $k_1 = m_1 \oplus c$ telle que $\mathsf{Enc}_{k_1}(m_1) = c$.
Puisque K est tiré uniformément dans $\{0,1\}^n$:

$$\Pr[\mathsf{Enc}_K(m_0) = c] = \Pr[K = k_0] = \frac{1}{2^n}$$
$$\Pr[\mathsf{Enc}_K(m_1) = c] = \Pr[K = k_1] = \frac{1}{2^n}$$

Donc $\Pr[\mathsf{Enc}_K(m_0) = c] = \Pr[\mathsf{Enc}_K(m_1) = c]$ pour tous m_0, m_1, c. Par la définition équivalente, le OTP a la sécurité parfaite. □ □

5.4 Exemple numérique

Exemple

OTP avec des bits

- Message : $m = 11010011$
- Clé (aléatoire) : $k = 10110101$
- Chiffrement : $c = m \oplus k = 01100110$
- Déchiffrement : $m' = c \oplus k = 01100110 \oplus 10110101 = 11010011 = m$ ✓

Observation : Sans connaître k, $c = 01100110$ pourrait correspondre à **n'importe quel** message de 8 bits avec égale probabilité !

6 Limitations de la sécurité parfaite

6.1 Théorème de Shannon

Malgré sa sécurité parfaite, le OTP est rarement utilisé en pratique à cause de limitations fondamentales prouvées par Shannon.

Théorème

Théorème de Shannon (1949)
Soit $(\mathcal{M}, \mathcal{K}, \mathcal{C}, \mathsf{Enc}, \mathsf{Dec})$ un système avec sécurité parfaite. Alors :

$$|\mathcal{K}| \geq |\mathcal{M}|$$

En particulier, si $\mathcal{M} = \{0,1\}^n$, alors $|\mathcal{K}| \geq 2^n$.
Conséquence : La clé doit être au moins aussi longue que le message pour avoir la sécurité parfaite !

Idée de la preuve. Supposons par l'absurde que $|\mathcal{K}| < |\mathcal{M}|$. Soit $c \in \mathcal{C}$ un ciphertext observé.
L'ensemble des plaintexts possibles pour c est :

$$\mathcal{M}_c = \{\mathsf{Dec}_k(c) : k \in \mathcal{K}\}$$

Puisque $|\mathcal{K}| < |\mathcal{M}|$, il existe au moins un $m^* \in \mathcal{M} \setminus \mathcal{M}_c$ qui ne peut jamais produire c avec aucune clé.
Donc $\Pr[\mathsf{Enc}_K(m^*) = c] = 0 \neq \Pr[\mathsf{Enc}_K(m) = c]$ pour $m \in \mathcal{M}_c$, ce qui contredit la sécurité parfaite. □ □

6.2 Conséquences pratiques

Le théorème de Shannon impose des contraintes rédhibitoires :

1. **Clés énormes** : Chiffrer 1 GB nécessite une clé de 1 GB !
2. **Distribution difficile** : Échanger de longues clés de manière sécurisée est un problème aussi difficile que d'échanger le message lui-même
3. **Usage unique** : Réutiliser la clé brise totalement la sécurité (voir section suivante)
4. **Pas de transmission multiple** : Chaque message nécessite une nouvelle clé de longueur égale

Avertissement

Impossibilité pratique
Pour la plupart des applications modernes (communication Internet, chiffrement de disques, etc.), la sécurité parfaite est **inapplicable**. C'est pourquoi la cryptographie moderne s'appuie sur la **sécurité computationnelle** (chapitre suivant).

6.3 Attaque par réutilisation de clé

La réutilisation de la clé OTP est catastrophique :

Exemple 6.1. ***Two-Time Pad Attack***
Supposons qu'Alice réutilise la même clé k pour chiffrer deux messages m_1 et m_2 :

$$c_1 = m_1 \oplus k$$
$$c_2 = m_2 \oplus k$$

L'adversaire observe c_1 et c_2. Il peut calculer :

$$c_1 \oplus c_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$$

Le XOR des deux plaintexts révèle beaucoup d'information ! Si les messages sont en anglais, on peut exploiter les fréquences des lettres, structures linguistiques, etc. pour retrouver m_1 et m_2.

***Exemple historique** : Le projet VENONA (1943-1980) a décrypté des milliers de messages soviétiques grâce à des réutilisations de clés OTP.*

7 Applications historiques

7.1 Téléphone rouge Moscou-Washington

Durant la Guerre Froide, le "téléphone rouge" (hotline) entre le Kremlin et la Maison Blanche utilisait le OTP pour les communications sensibles :

— Clés pré-distribuées physiquement par valise diplomatique

— Machines de chiffrement spécialisées (ex : ETCRRM)

— Destruction sécurisée des clés après usage

— Génération de clés par processus physiques aléatoires (bruit thermique)

7.2 NSA et renseignement

La NSA a utilisé (et utilise probablement encore) le OTP pour :

— Communications avec agents en territoire hostile

— Messages ultra-sensibles de niveau présidentiel

— Systèmes de commande nucléaire

Ces usages sont justifiés car :

— Volumes de données faibles (messages courts)

— Budget illimité pour la distribution de clés

— Enjeux de sécurité absolus

8 Travaux dirigés

8.1 Exercices théoriques

1. **Sécurité du chiffre de César**
   Montrer formellement que le chiffre de César n'a pas la sécurité parfaite.
2. **Variante du OTP**
   Considérer le système suivant sur $\{0,1\}^n$:
   $\mathsf{Enc}_k(m) = (m \oplus k) \parallel k$
   où $\parallel$ dénote la concaténation. Ce système a-t-il la sécurité parfaite ? Pourquoi ?
3. **OTP avec clé courte**
   Soit $m \in \{0,1\}^{2n}$ et $k \in \{0,1\}^n$ avec $|k| = n < 2n = |m|$. On définit :
   $\mathsf{Enc}_k(m) = m \oplus (k \parallel k)$
   (la clé est répétée). Montrer que ce système n'a pas la sécurité parfaite.
4. **Indistinguabilité**
   Montrer l'équivalence entre les deux définitions de la sécurité parfaite données en section 4.
5. **Borne inférieure sur $|\mathcal{C}|$**
   Montrer que si un système a la sécurité parfaite, alors $|\mathcal{C}| \geq |\mathcal{M}|$.

8.2 Exercices pratiques

Les notebooks suivants implémentent et explorent les concepts de ce chapitre :

— $01_demo_otp.ipynb$: $ImplmentationduOne-TimePad$

- $01_demo_xor_properties.ipynb$: $ExplorationdespropritsduXOR$

- $01_exercices.ipynb$: $Exercicespratiquesguids$

Exercices proposés :

1. Implémenter OTP et vérifier la correction
2. Two-Time Pad attack : casser des messages réutilisant la clé
3. Statistiques : vérifier expérimentalement l'uniformité de $m \oplus k$
4. Attaque par fréquence des lettres sur messages chiffrés avec clé réutilisée

9 Ressources complémentaires

9.1 Références

— **Article fondateur** : Shannon, C. E. (1949). "Communication Theory of Secrecy Systems". Bell System Technical Journal, 28(4), 656-715.

— **Livre de référence** : Rosulek, M. (2021). "The Joy of Cryptography", Chapitre 2. https://joyofcryptography.com/pdf/book.pdf

— **Cryptographie moderne** : Katz, J., & Lindell, Y. (2020). "Introduction to Modern Cryptography" (3e éd.). CRC Press.

— **Projet VENONA** : NSA. "The VENONA Story". https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/venona/

9.2 Cours en ligne

— Coursera : "Cryptography I" par Dan Boneh (Stanford)

— MIT OpenCourseWare : 6.857 Computer and Network Security

— Christof Paar : Introduction to Cryptography (YouTube)

10 Conclusion

Ce chapitre a posé les fondations de la cryptographie moderne :

— Les principes de Kerckhoffs restent valides aujourd'hui

— La sécurité parfaite de Shannon est une notion théorique forte mais impraticable

— Le One-Time Pad est le seul système prouvé parfaitement sécurisé

— Le théorème de Shannon impose des limites fondamentales : $|\mathcal{K}| \geq |\mathcal{M}|$

— En pratique, on abandonne la sécurité parfaite pour la sécurité computationnelle

Le chapitre suivant introduira les **chiffrements par flot et par bloc**, qui relaxent l'exigence de sécurité parfaite pour obtenir des systèmes pratiques avec des clés courtes réutilisables, au prix d'hypothèses de calcul (difficulté de certains problèmes algorithmiques).

"The enemy knows the system."
— Claude Shannon, citant Auguste Kerckhoffs