

# Introduction à la Sécurité

---

## 1.1 Objectifs de la sécurité

La sécurité vise à assurer plusieurs propriétés :

**La confidentialité** : c'est la propriété qui garantit que les informations transmises ne sont compréhensibles que par les entités autorisées.

**L'authentification** : c'est la propriété qui consiste à vérifier l'identité d'un utilisateur avant de lui donner l'accès à une ressource.

**L'intégrité** : c'est la propriété qui consiste à vérifier si les informations n'ont pas été modifiées durant la transmission.

**La disponibilité** : c'est la propriété qui permet de garantir l'accès aux données.

**La non-répudiation** : c'est la propriété qui permet d'avoir une preuve comme quoi un utilisateur a envoyé (ou reçu) un message particulier. Cette propriété permet d'empêcher l'utilisateur de nier l'envoi (ou réception) du message en question.

## 1.2 Les scénarios d'attaques

### 1.2.1 Attaque passive

Dans ce genre d'attaques, les informations ne sont pas modifiées. L'attaquant collecte seulement les informations qui circulent sur le réseau.

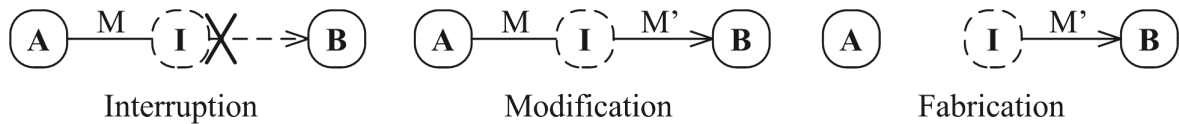
### 1.2.2 Attaque active

Il y a trois cas possibles pour mener une attaque active :

**L'interruption** : l'intrus intercepte le message envoyé par l'utilisateur  $\mathcal{A}$  pour  $\mathcal{B}$  et l'interrompt.

**La modification :** l'intrus intercepte le message envoyé par l'utilisateur  $\mathcal{A}$  et le modifie avant de le faire suivre à l'utilisateur  $\mathcal{B}$ .

**La fabrication :** L'intrus fabrique un message et l'envoie à l'utilisateur  $\mathcal{B}$  en se passant pour l'utilisateur  $\mathcal{A}$ .



## 1.3 Concepts de base sur la cryptographie

**Chiffrement et déchiffrement :** consiste à transformer une donnée afin de la rendre incompréhensible par un utilisateur autre que celui qui l'a créée et celui qui va la recevoir.

**Chiffré :** c'est le résultat de chiffrement d'une donnée.

**Clé :** il s'agit d'un paramètre impliqué dans les opérations de chiffrement et de déchiffrement et qui est partagé entre l'émetteur et le récepteur.

**Cryptanalyse :** elle a pour but de retrouver la donnée en claire à partir d'un ou plusieurs chiffrés sans connaître les clés et/ou l'algorithme de chiffrement.

**Canal :** moyen de transport de l'information.

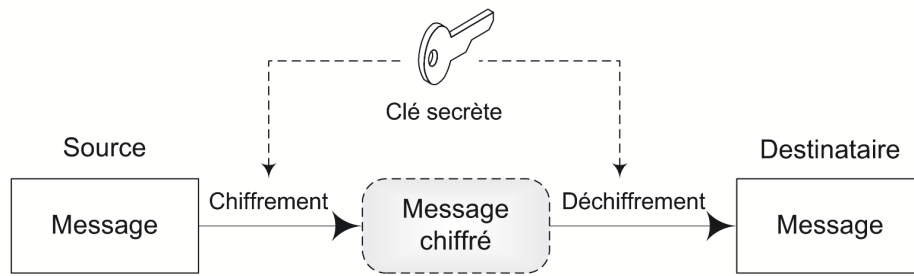
**Canal sécurisé :** canal où l'intrus n'a pas la possibilité d'altérer les messages.

**Canal sécuritaire :** canal qui n'est pas physiquement accessible à l'intrus.

## 1.4 Les algorithmes cryptographiques

### 1.4.1 Algorithmes à clés symétriques

Dans ce type d'algorithme, la même clé est utilisée à la fois pour le chiffrement et le déchiffrement (DES, AES, IDEA, ... etc.).

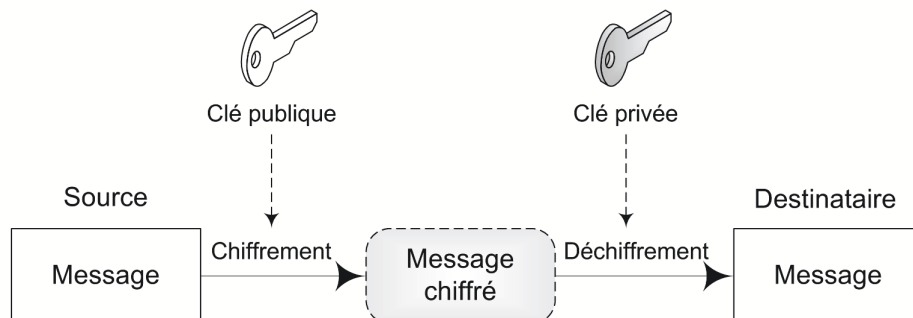


#### 1.4.1.1 Exemple

- ★ Le message  $\mathcal{M} = 139$ .
- ★ L'opérateur de chiffrement et de déchiffrement :  $\oplus$  (XOR).
- ★ La clé  $\mathcal{K} = 199$ .
- ★  $\mathcal{C} = \mathcal{M} \oplus \mathcal{K} = 139 \oplus 199 = 76$ .
- ★  $\mathcal{M} = \mathcal{C} \oplus \mathcal{K} = 76 \oplus 199 = 139$ .

#### 1.4.2 Algorithmes à clés asymétriques

Dans ce type d'algorithmes, chaque entité possède une paire de clés : *publique* et *privée*. La clé publique est utilisée pour le chiffrement et la clé privée pour le déchiffrement (RSA, Elgamal, Rabin, Merkel-Hellman, ... etc.).



La signature numérique consiste à générer un condensé à partir d'un message et le chiffrer en utilisant la clé privée de l'émetteur. Ce dernier, ensuite, envoie le message en clair avec la signature. Pour vérifier la validité de cette signature, le récepteur recalcule le condensé à partir du message en clair et déchiffre la signature. Ensuite, il vérifie l'égalité des deux résultats.

### 1.4.3 Fonctions de hachage

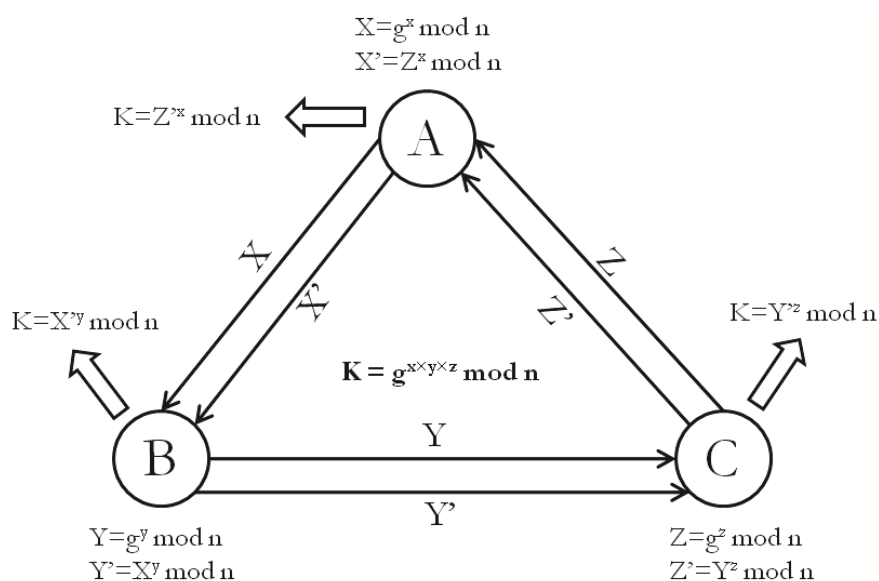
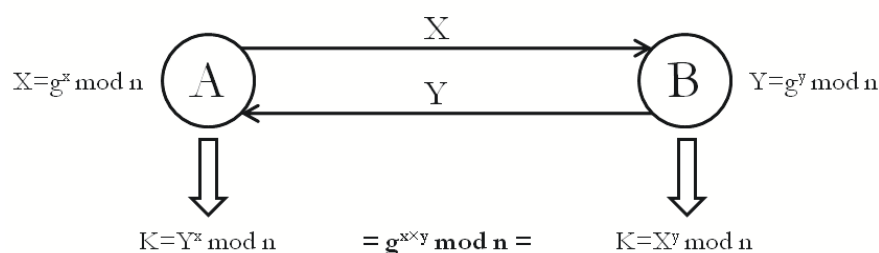
Il s'agit de la troisième famille d'algorithmes cryptographiques. Le principe est qu'un message  $\mathcal{M}$  de longueur quelconque est transformé en une valeur  $h$  de longueur fixe et inférieure à celle du départ ( $h = H(\mathcal{M})$ ) et qui représente d'une manière unique le message  $\mathcal{M}$ . Deux caractéristiques importantes sont les suivantes :

1. A partir de  $h$ , il est impossible de retrouver  $\mathcal{M}$ .
2. Etant donné  $h = H(\mathcal{M})$ , il est impossible de trouver  $\mathcal{M}'$  tel que  $H(\mathcal{M}') = h$ .

# Algorithmes de Chiffrement à Clés Publiques

## 2.1 Protocole de Diffie-Hellman

Le protocole d'échange de Diffie-Hellman est une méthode par laquelle deux utilisateurs peuvent partager une clé de chiffrement symétrique. Le protocole tire sa sécurité du problème du Logarithme discret. Il peut s'exécuter avec deux ou plusieurs utilisateurs.



## 2.2 Chiffrement de RSA

L'algorithme de chiffrement de RSA tire sa sécurité du problème de factorisation des grands nombres entiers. L'algorithme se déroule en trois étapes :

1. *Création de clés* : On choisit deux nombres premiers  $p$  et  $q$  et on calcule  $n$  et  $\phi(n)$  tels que  $n = p \times q$  et  $\phi(n) = (p - 1) \times (q - 1)$ . Ensuite, on choisit  $e < \phi(n)$  tel que  $\text{pgcd}(e, \phi(n)) = 1$ , et enfin on calcule  $d$  tel que  $e \times d \bmod \phi(n) = 1$ . La clé publique est  $(e, n)$  et la clé privée est  $(d, n)$ .
2. *Chiffrement* : Le message à chiffrer doit être strictement inférieur à  $n$ . Pour chiffrer un message  $\mathcal{M}$ , on calcule  $\mathcal{C} = \mathcal{M}^e \bmod n$ .
3. *Déchiffrement* : Pour déchiffrer le message, on calcule  $\mathcal{M} = \mathcal{C}^d \bmod n$ .

### 2.2.1 Exemple

- ★  $p = 19, q = 23 \Rightarrow n = 19 \times 23 = 437$  et  $\phi(n) = (19 - 1) \times (23 - 1) = 396$ .
- ★  $e = 17 \Rightarrow 17d \bmod 396 = 1 \Rightarrow d = 233$ .
- ★ Pour  $\mathcal{M} = 351 \Rightarrow \mathcal{C} = 351^{17} \bmod 437 = 150$ .
- ★  $\mathcal{M} = 150^{233} \bmod 437 = 351$ .