Chiffrement et Déchiffrement.

Le **chiffrement** (ou **cryptage**) est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

Mais d'autres techniques peuvent être utilisées pour communiquer de façon sûre. Par exemple : Pour vérifier l'intégrité ou l'authenticité d'un document, on peut utiliser soit un *Message Authentication Code (MAC)* ou bien une signature numérique.

La sécurité d'un système de chiffrement doit reposer sur le secret de la clé de chiffrement et non sur celui de l'algorithme. Le principe de Kerckhoffs suppose en effet que l'attaquant connaisse l'algorithme utilisé pour le chiffrement .

Système symétrique ou asymétrique

Un système de chiffrement est dit :

- à chiffrement symétrique quand il utilise la même clé pour chiffrer et déchiffrer ;
- à chiffrement asymétrique quand il utilise des clés différentes : une paire composée d'une *clé publique*, servant au chiffrement, et d'une *clé privée*, servant à déchiffrer.

Les méthodes de chiffrement les plus connues sont le DES, le Triple DES et l'AES pour le chiffrement symétrique, et le RSA pour le chiffrement asymétrique, aussi appelé chiffrement à clé publique.

L'utilisation d'un système symétrique ou asymétrique dépend des tâches à accomplir.
La cryptographie asymétrique présente deux intérêts majeurs : elle supprime le problème de transmission sécurisée de la clé, et elle permet la signature électronique.

Exemple de choix de cryptage de transactions bancaires.

En 1977 pour la sécurisation des transmissions bancaires nous avons fait le choix d'une solution de chiffrage DES avec partage de clef.

Apres la première transaction la clef de cryptage était changée pour moitié à chaque nouvelle transaction. Cette moitié était mixée avec la moitié de l'ancienne clef pour créer une nouvelle clef. Et a la transaction suivante le processus recommençait.

Mais pour diminuer le temps de cryptage décryptage nous avons seulement crypté la partie de chaque transaction qui contenait des informations spécifiques aux données bancaires (nom, numéro de la carte etc..) mais pas la totalité des messages.