# LA CRYPTOGRAPHIE

## Qu’est-ce que le chiffrement ?

Le chiffrement est une technique de cryptographie qui a pour but de protéger ses données les rendant ainsi incompréhensible/ illisible par quiconque ne disposant pas de la clef de déchiffrement.

En Informatique le chiffrement sert à garantir la confidentialité des données stockées sur des systèmes informatiques ou en transit. Les données sont chiffrées à l’aide d’un algorithme et d’un jeu de clef de chiffrement. Le chiffrement apporte une valeur de confidentialité et d’intégrité aux données

**Comment s’assurer qu’un espion ne lise pas le contenu de nos communications sur internet ?**

Les communications sur internet sont loin d’être sûres et au-delà du bon comportement et de la méfiance que l’on peut apporter à l’égard d’internet et de son utilisation il reste toujours des risques que quelqu’un intercepte vos données ou vos échanges.

On va alors parler de **Cryptographie** :

La cryptographie ou encore le chiffrement, s’effectue avec le protocole TLS (transport layer Security) ce qui représente “s” de HTTPS

Il existe deux types de chiffrement :

- Le chiffrement symétrique

- Le chiffrement asymétrique

## Quelques notions essentielles :

### Le certificat

Le certificat est un fichier qui contient

- Numéro de série
- Nom/prénom/entreprise
- Émetteur
- Date de validité (max 1 ou 2 ans)
- Clé publique
- Objet
- Fonction de hachage
- Condensat

**La date de validité** et mise en place pour contrer les attaques de force brute

Émetteur organisme qui va vérifier et va jurer sur son honneur que oui ce certificat est celui de bob je m’y engage

**Les PKI :**

Ces organismes sont des PKI (public key infrastructure / infrastructures à clé publique)

Il existe 4 catégories de PKI selon L'IETF :

- L'autorité d'enregistrement
- Autorité de certification
- Autorité de dépôt
- Entité d'extrémité

Les PKI ça peut être soit 1 de la liste mais aussi les 4 à la fois

*une autorité de certification peut être certifié par une autre autorité de certification et ca peut durer longtemps, on appelle ca une chaîne de confiance et ça va s'arrêter par une* ***autorité de certification racine***

Les racines sont les grands noms d'autorité, on peut se fier à elles.

**Un peu de vocabulaire :**

- **Confidentialité** : les données (et l'objet et les acteurs) de la communication ne peuvent pas être connues d'un tiers non-autorisé.
- **Intégrité** : les données de la communication n'ont pas été altérées.
- **Disponibilité** : les acteurs de la communication accèdent aux données dans de bonnes conditions 24/24H et 7/7J. La disponibilité comprend pour une entreprise de toujours avoir un double des informations au cas où il y aurait une panne technique la deuxième machine prendrait le relais.
- **Non répudiation** : Les acteurs impliqués dans la communication ne peuvent pas nier y avoir participé.
- **L'Authentification** : l'identité des acteurs de la communication est vérifiée. Ce peut être à travers un identifiant et un mot-de-passe
- **Certificat** : preuve d'un fait, d'un droit accordé.

**Tiers de confiance** : personne physique ou morale habilitée à effectuer des opérations de sécurité juridique d'authentification, de transmission et de stockage.

## 1) Le chiffrement symétrique :

### A- Le code de césar

Le principe du code de césar est de prendre un message et de décaler les lettres de quelques crans dans l'alphabet.

Exemple : avec un décalage de 2 lettres (clé de chiffrement)

"le message" devient -> "ng oguucig"

Ce chiffrement est dit **symétrique** car l'information de chiffrement, le décalage (que l'on appelle la clé) permet aussi bien de chiffrer que de déchiffrer. Elle est utilisée par l'envoyeur pour crypter et par le receveur pour décrypter.

Mais cette méthode est déchiffrable avec la méthode de la cryptanalyse.

La cryptanalyse est l'ensemble des méthodes mises en œuvre pour tenter de déchiffrer un message codé dont on ne connaît pas la clé.

On trouve aussi d'autres techniques de chiffrement asymétrique que l'on ne détaillera pas comme :

- Block Ciphers
- Stream Ciphers

B- Les types d'attaque :

- La force brute ou attaque exhaustive : (le plus basique)

  Consiste à essayer toutes les combinaisons possibles

- L'attaque à texte chiffré seul :

  On ne dispose que d'un ou de plusieurs messages chiffrés, sans avoir d'informations sur leur signification en clair.

- L'attaque à texte clair continu :

  L'attaquant possède plusieurs paires du type message clair/message codé.

- L'attaque à texte clair choisi :

  L'attaquant choisit lui-même le message à coder.

- L'attaque par mot probable :

  On ne connaît pas tout le message clair, mais au moins une partie, par exemple, la signature, ou bien le début, etc…

**2) Le chiffrement asymétrique :**

C- Le chiffrement AES et RSA :

Pour échapper à la cryptanalyse il faut que le chiffrement ait l'air aléatoire. Aujourd'hui on utilise des chiffrements symétriques assez complexe mais rapides tel que AES (Advanced Encryptions Standard) permet d'obtenir un msg chiffré suffisamment aléatoire pour que sans clé de chiffrement on ne puisse pas le décrypter sauf en essayant toute les clé possible (technique de force brute) mais cela prendrait beaucoup trop de temps (on estime en années). Le problème du chiffrement symétrique est qu'il faut transmettre la clé secrète pour que le receveur puisse décrypter les messages mais celle-ci pourrait être interceptée durant son envoi et ainsi les échanges ne seraient plus sécurisés.

**Chiffrement asymétrique**

Cette technique de chiffrement est plus sûre mais aussi beaucoup plus lourde et plus longue que le chiffrement symétrique.

La méthode RSA (Ronald Rivest, Adi Shamir et Leonard Adleman) utilise des propriétés des nombres premiers, elle permet d'avoir

- Une clé pour chiffrer (clé publique)
- Une clé pour déchiffrer. (Clé privée)

**un exemple en situation avec Bob et Alice deux correspondants:**

Les personnes peuvent échanger leur clé publique librement tant qu'ils conservent leur clé privée non accessible par autrui.

Ainsi deux personnes Alice et Bob peuvent communiquer de manière sécurisée.

Alice chiffre le document à envoyer avec sa clé privée puis l'envoie et Bob le décrypte avec la clé publique d'Alice pour pouvoir le lire en clair

Le problème de cette méthode est la possibilité d'interception par un tiers aussi appelé, "**man in the middle**" qui consiste à intercepter des informations ou des documents en transaction entre Alice et Bob par exemple en captant le réseau wifi.

Pour pallier ce défaut il est possible d'utiliser le **chiffrement asymétrique à 2 clés.** Considérons Alice possédant 2 clés (une privée et une publique) de même pour Bob.

Ainsi pour qu'a envoie un document à Bob il devra d'abord crypter le document à envoyer avec la clé publique de Bob puis crypter avec sa propre clé privée (clé de Alice).

Aussi pour décrypter le document, Bob devra d'abord utiliser la clé publique de Alice puis avec sa clé privée

**Une communication sécurisée va fonctionner ainsi**

1. Envoie du message en clair avec la liste des algorithmes que l'on peut utiliser (RSA+AES ou RSA + DES)
2. Le site répond par exemple RSA + AES et envoie son certificat qui contient sa clé publique et d'autres informations essentielles.
3. Ensuite envoie de la clé AES, en crypté par le chiffrement RSA au destinataire.
4. Celui-ci nous répond que tout est ok
5. Les échanges sécurisés peuvent ainsi débuter.

*La suite des échanges après réception se fait par le chiffrement symétrique car c'est la solution la plus rapide et la plus simple. Le chiffrement RSA en plus d'être long, augmente la taille des fichiers ce qui n'est pas négligeable pour de gros fichiers qui les rendaient encore plus lourds et donc plus long à envoyer.*

On note aussi d'autre chiffrements symétriques comme le Chiffrement de Vernam qui sont beaucoup plus complexe et qui sans la clé est indéchiffrable dans un temps raisonnable

**Tableau comparatif des 2 méthodes**

| //// | avantages | inconvénients |
|---|---|---|
| symétrique | - Chiffrement rapide | - Il faut envoyer la clé au destinataire ce qui représente un danger quant à la confidentialité des échanges |
| Asymétrique | - Chiffrement solide<br>- Deux clé et authentification de son interlocuteur | - Le chiffrement rend les documents plus lourds<br>- Le chiffrement est plus long |