Chiffrement Informatique et Sécurité Informatique

I► Dans cet article, nous allons aborder le chiffrement ou encryptage des données Informatiques.

Le chiffrement Informatique permet de rendre illisible un document informatique quelque soit son format. Afin de pouvoir lire le document, il est nécessaire de posséder une clé de chiffrement et dans ce cas là l'utilisateur peut **déchiffrer** ce document. On parle de **décryptage** quand on rend lisible le document sans posséder la fameuse clé de chiffrement.

Il existe 2 systèmes de chiffrements à clés :

- **Chiffrement symétrique** : La même clé est utilisée pour encrypter et décrypter les données.
- **Chiffrement asymétrique** : On utilise cette fois-ci 2 clés (clé publique et clé privée) qui permettent de crypter et décrypter les données en offrant une performance plus élevée.

Pour encrypter les données, la clé est crée en utilisant un algorithme d'encryptage. Dans le cas du chiffrement symétrique, l'algorithme **AES** est utilisé mais on peut trouver d'autres types d'algorithme tels que DES.

Advanced Encryption Standard est un algorithme dont la clé peut être codée sur 128, 192 256 Bits. AES 256 peut donc créer des clés avec un nombre de possibilités égal à 2^{256}= **1.16×10^{77} , soit un nombre composé de 77 chiffres** ! Il est donc quasiment impossible d'attaquer cette clé par force brute* et de tester toutes les combinaisons possibles et inimaginables.

*Une attaque par force brute permet de déchiffrer un mot de passe ou une clé de chiffrement en testant toutes les combinaisons possibles. Il faut donc du temps pour tester

toutes ces combinaisons et plus la clé ou le mot de passe est complexe et plus l'attaque sera sans effet.

☼ Le principe du chiffrement asymétrique :

Le chiffrement asymétrique repose sur un système composée de 2 clés :

- La clé **publique** (véhiculée sur le réseau informatique) et qui permet de **chiffrer** les données.
- La clé **privée** (qui reste sur le terminal de l'utilisateur) et qui permet de **déchiffrer** ces mêmes données.

Voici un exemple simple pour bien comprendre le processus :

1. Le détective envoie à son client un attaché-case avec cadenas (la clé publique) à code secret (la clé privée) et lui demande d'y placer les documents confidentiels
2. Le client s'exécute et ferme le cadenas sans connaître son code !
3. Le client renvoie l'attaché-case au détective qui lui peut ouvrir le cadenas !

A aucun moment, le code (la clé privée) n'a fait partie du voyage..
Le cadenas (la clé publique) lui a parcouru le chemin détective-client client-détective.

Voici un schéma d'une transaction HTTPS :

L'algorithme **RSA** du nom de ses inventeurs Ronald **R**ivest, Adi **S**hamir et Leonard **A**dleman est un algorithme de chiffrement asymétrique très utilisé dans le monde d'Internet et du paiement en ligne et de la protection des données. C'est un puissant algorithme mathématique. Il permet de générer des clés codées sur plusieurs centaines voire milliers de bits.

RSA 2048 permet donc de créer des combinaisons de 2^{248}, soit

3.23×10^{616} des nombres composés de **617 chiffres** !

Voici l'exemple du certificat d'un site Internet utilisant cet algorithme pour sécuriser les transactions :

Notre ami Google lui utilise un algorithme de chiffrement asymétrique beaucoup plus récent que RSA :

Il s'agit de l'agorithme **ECC : Elliptic Curve Cryptography.**
ECC est 12 fois plus puissant que RSA : un chiffrement 2048 bits en RSA correspond à un chiffrement 256 bits en ECC.

ECC génère des clés publiques beaucoup plus courtes ainsi les connexions seront plus rapides. De nos jours ou la consommation Internet se fait principalement par les terminaux mobiles (Smartphones et tablettes), cela a évidement un grand intérêt.

Michel BOCCIOLESI