Première année

Cours 3: La cryptographie

La confidentialité est importante dans de nombreux domaines: militaire, commercial, bancaire, diplomatique et vie privée.

Cryptologie – > signifie littéralement "*science du secret*", elle comprend:

- **la cryptographie**: l'étude des écritures secrètes
- **la cryptanalyse**: le déchiffrement d'un message sans en avoir la clé
- **la stéganographie**: l'art de la dissimulation

Cryptographie – > sert à **assurer la protection de messages**: elle assure leur intégrité, authenticité et leur confidentialité

Chiffrement – > procédé de la cryptographie (méthode): **permet de rendre incompréhensible un document sauf si on possède la clé de (dé)chiffrement**

/!\ NE PAS CONFONDRE **déchiffrement** et **décryptage**

déchiffrement – > déchiffrer un message en **possédant la clé** de (dé)chiffrement

décryptage – > méthode pour déchiffrer un message **sans posséder la clé** de (dé)chiffrement

Chronologie des méthodes

Ve siècle avant JC	Ier siècle avant JC	1586
Les Spartiates	Jules César	Blaise de Vigenère
Un **bâton de bois** autour duquel il y a un message: il faut avoir un 2ème bâton pour déchiffrer	**Méthode de substitution:** décaler les lettres de l'alphabet d'un nombre n de cases, il faut connaître "n" pour pouvoir déchiffrer.	**Méthode de substitution polyalphabétique:** une même lettre peut, suivant sa position dans le message, être remplacée par des lettres différentes.

1942	1977	2000
Alan Turing	Adi Shamir, Roland Rivest et Leonard Adleman	Vincent Rijmen et Joan Daemen
Fabrique un **système** capable de **décrypter la machine Enigma** utilisée par l'armée allemande pour crypter ses messages.	Inventent **l'algorithme RSA**, 1er système de cryptographie associant une clef publique et une clef privée. Utilisée aujourd'hui pour les systèmes de paiement.	Créent **l'algorithme AES**, qui est à ce jour le plus solide système de cryptographie symétrique: pour en venir à bout, il faut effectuer 10^{77} opérations.

Les méthodes courantes:

- par substitution
- par transposition (permutation)

Le chiffre de César – > **décalage des lettres de l'alphabet de nombre n** (*méthode de substitution monoalphabétique*)

Le chiffre de Vigenère – > *chiffrement polyalphabétique par bloc*, l**e texte clair est chiffré à l'aide d'une clé constituée de n nombres**.

Chiffrement à clé asymétrique – > créer une *fonction à sens unique*: on peut **facilement chiffrer le message à l'aide d'une clé mais difficilement le déchiffrer sans avoir la deuxième clé**.

Chiffrement RSA – > *cryptographie associant une clef publique et une clef privée*: **la clef publique pour chiffrer le messager et la clef privée pour déchiffrer ce message**. **Exemple**: Si Bruno veut envoyer un message secret à Alice – >

1) Alice prépare deux clés: clef publique et clef privée.

2) Bruno utilise la clef publique d'Alice pour chiffrer son message

3) Alice reçoit le message chiffré et le déchiffre grâce à sa clef privée.