Chapitre 2 : Cryptographie Symétrique Classique

1) Modèle de chiffrement symétrique

On distingue 2 types d'échange :

- Echange de la clé secrète : .....
- Echange des données chiffrées : .....

2) Attaques

L'objectif principal d'un attaquant est de trouver la clé de chiffrement et non pas le message en clair correspondant à un seul message chiffré. Il y a deux types d'attaques pour atteindre cet objectif :

- **La cryptanalyse** : consiste à exploiter les caractéristiques de l'algorithme et du texte pour déduire le message en clair ou la clé de chiffrement (cette attaque n'est pas toujours possible).
- **Attaque par force brute** : l'attaquant essayes toutes les clés possibles sur un message chiffré jusqu'à trouver le message en clair (en moyenne la moitié de toutes les clés possibles doit être essayée pour trouver la bonne clé).

3) Techniques classiques de chiffrement

Ces techniques sont apparues avant et au début de l'ère des ordinateurs. Elles ont cédé la place à des algorithmes modernes plus puissants. Les techniques classiques sont classées en 2 catégories principales :

- **Techniques de substitution** : remplacent les lettres d'un message par les lettres chiffrées correspondantes. **Exemples** : Algorithme de César, Chiffrement Mono-alphabétique, Playfair, Vigenère, Vernam.
- **Techniques de permutation** : changent l'emplacement des lettres dans un message pour obtenir le message chiffré. **Exemple** : Rail Fence

4) Algorithme de César

L'algorithme de base remplace chaque lettre par une lettre située 3 emplacements plus loin dans l'alphabet : c'est un chiffrement par décalage circulaire des lettres.

Exemple 1 :

```
Clair   : a b c d e f g h i j k l m n o p q r s t u v w x y z
Chiffré : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Exemple 2 :

```
Clair   : faculte des sciences de monastir
Chiffré : ....... ... ........ .. ........
```

La clé de l'algorithme de César correspond au nombre de décalage. L'algorithme de base utilise la clé « 3 ». En générale, la clé peut avoir n'importe quelle valeur de 1 à 25 (pour un alphabet de 26 lettres). Si l'attaquant sait qu'un message est chiffré par l'algorithme de César, une attaque par force brute permet de déterminer la clé facilement.

Exercice : Trouver la clé utilisée pour chiffrer le message « **RJXXFLJ HTSKNIJSYNJQ** » et déduire le message en clair.

5) Chiffrement mono-alphabétique

Le chiffrement mono-alphabétique utilise une substitution aléatoire, tel que :

- Une lettre chiffrée correspond à une seule lettre claire (n'importe laquelle)
- La clé permet de déterminer la correspondance entre les lettres claires et chiffrées

Exemple 1 :

```
Clair           : abcd efgh ijkl mnop qrst uvwx yz
Chiffré (clé)   : DKVQ FIBJ WPES CXHT MYAU OLRG ZN
```

Exemple 2 :

```
clair   : bonjour
chiffré : .......
```

Un alphabet de 26 lettres possède ..... clés possibles. Ainsi, une attaque par force brute impossible. Mais cette approche est vulnérable à une attaque par cryptanalyse : si l'attaquant connaît la nature et la langue du texte en clair, il peut exploiter la fréquence des lettres de la langue pour déchiffrer le message et trouver la clé.

6) Playfair

L'algorithme Playfair utilise une matrice 5X5 construite en utilisant la clé secrète. Cette matrice est remplie par les lettres de la clé, déduction faite des doubles (exemple : **informatique** devient **informatque**), de gauche à droite et de haut en bas. Les cases restantes de la matrice sont remplies avec les lettres restantes dans l'ordre alphabétique (les lettres `I` et `J` comptent pour une seule lettre).

Exemple (matrice Playfair avec la clé informatique) :

Le message en clair est chiffré **par groupes de 2 lettres**, selon les règles suivantes:

- 2 lettres identiques appartenant à la même paire seront séparées en ajoutant une lettre de remplissage au milieu. **Exemple** : **ballon → ba lx lo nx**
- 2 lettres qui se trouvent dans la même ligne de la matrice seront décalées une case vers la droite. **Exemple** : **au → TM**
- 2 lettres qui se trouvent dans la même colonne seront décalées une case vers le bas. **Exemple** : **po → YQ**
- Pour toutes les autres paires « $l_1 l_2$ » :
    - l_1 sera remplacée par la lettre qui se trouve dans la ligne de l_1 et la colonne de l_2
    - l_2 sera remplacée par la lettre qui se trouve dans la ligne de l_2 et la colonne de l_1s **Exemple** : **ad → QB**

Exercice

a) Donner la matrice Playfair de la clé « sécurité »
b) Chiffrer le message « information confidentielle »
c) Déchiffrer le message « HIURGDCW TRCV EUTSOECE »

7) Rail Fence

Contrairement aux algorithmes précédents, la technique « Rail Fence » consiste à permuter l'emplacement des lettres du message original pour obtenir un message chiffré. Pour chiffrer un message on procède comme suit :

- On écrit le message de haut en bas, sur plusieurs colonnes d'une matrice
- Quand on atteint la dernière case d'une colonne, on passe à la première case de la colonne suivante
- Lorsqu'on termine l'écriture du message, on remplit la dernière colonne avec des lettres de remplissage : « X »
- On obtient le message chiffré en lisant la matrice ligne par ligne
- Le nombre de lignes de la matrice représente la profondeur (P) du « Rail Fence », et **correspond à la clé**.

Exemple : chiffrer le texte « **`message confidentiel`** » avec Rail Fence et P = 4

Pour déchiffrer :

- On calcule le nombre de lettres du message chiffré : N
- On divise ce nombre par « P » pour obtenir le nombre de colonnes : C = N/P
- On remplit la matrice **ligne par ligne** et on lit le texte **colonne par colonne**

Exercice : déchiffrer le message « SUTNRTUEREFMIECIIOAQX » sachant que P = 3

Remarque : Il est possible de casser cette technique avec une attaque de type force brute en essayant toute les valeurs possibles de P.

Pour renforcer la sécurité de « Rail Fence », il est possible de permuter l'ordre des lignes : cet ordre devient la clé de chiffrement

Exemple :

Clé	Texte clair
7	U O A I L E L V L
4	N N G D C P F E E
2	T G E E H A E C X
3	R M C N I R N U X
6	E E O T F R C N X
1	S S N I F A E E X
5	L S F E R I A C X

Clé : 7423615

Texte chiffré :

SSNIFAEEXTGEEHAECXRMCNIRNUXNNGDCPFEELSFERIACXEEOTFRCNXUOAILELVL