Centre universitaire - Salhi Ahmed - de Naâma

Institut des Sciences et de la Technologie
Département : Mathématiques et Informatique
3ème Année Licence Informatique
Matière : Sécurité Informatique

Fiche TD : 02

Exercice 01 : Expliquer les termes suivants :

Cryptographie, Stéganographie, cryptologie, cryptanalyse, cryptogramme, chiffrer (crypter), déchiffrer, clé.

Exercice 02 : Substitution mono-alphabétique

Le tableau suivant montre les caractères alphabétiques du français standard et les entiers correspondants :

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*
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 1 : Table de correspondance

Soit M = **CRYPTOLOGIEMODERNE** le message en clair et K = 3 (Chiffre de Jules César) la clé de chiffrement.

1) Chiffrez le message en clair M.
2) Déchiffrez le message chiffré (résultat de la question précédente).
3) Quelle remarque peut-on tirée entre le message M et le message chiffré ?

Exercice 03: Chiffrement de Vigenère

1) Chiffrer à l'aide de l'algorithme de Vigenère le texte suivant : **textesecretadecoder** en utilisant comme clé le mot **crypto**.
2) Pour le même texte clair, on obtient le texte chiffré suivant **brqksmzcspxiqxtcxzr**. Quelle est la clé ?
3) Même question si le chiffré est **aaabbbcccdddeeefffg**. Que remarque-t-on ?

Exercice 04 : Le nombre de clés disponibles dans un système de chiffrement donne une borne maximale de sa sécurité (Mesure de la complexité d'une recherche exhaustive).

1) Quel est le nombre de clés possibles pour un chiffrement de César ?
2) Pour un chiffrement par substitution (substitution arbitraire, caractère par caractère) ?
3) Pour un chiffrement affine ? ($C(x) = ax + b \bmod 26$ pour chaque caractère $x \in Z_{26}$)
4) Pour un chiffrement de Vigenère (avec une clé de longueur k) ?