Université Echahid Hamma Lakhdar-El-oued

Faculté des sciences exactes

3ème année licence informatique

Sécurité informatique

TD N°2

Exercice 1:

Déchiffrer les messages suivants selon Hill $M = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$

« OUBVN MKCU HJADZ TMJBGZMKNN»

Déchiffrer les messages suivants selon Hill $M = \begin{pmatrix} 5 & 2 \\ 4 & 3 \end{pmatrix}$

« VCUDJSBIUQ»

Exercice 2:

Chiffrer les messages suivants par transposition avec la clé = salut.

« une excellente vacance»

Déchiffrer les messages suivants par transposition avec la clé = grain.

« SJUIE VSECA UVSXO »

Exercice 3:

1- Créer un pair de clé en utilisant le protocole RSA si p = 47, q = 59, e =17 pour chiffrer le message m= 66.
2- Même question pour p = 29, q = 31, e =13 et m = 123.

Exercice 4:

Effectuer un protocole d'échange de clé Diffie-Hellman et obtenir la clé secrète dans les cas suivants :

1- Alice et Bob partagent p = 233 et g = 45, Alice choisit a = 11 et Bob b = 20.
2- Alice et Bob partagent p = 23 et g = 3, Alice choisit a = 6 et Bob b = 15.