ENSIAS 14-15

TD –Cryptographie : Série 1

1- Chiffre RSA :

Un message M a été chiffré avec la clé publique (n =943 , e = 19) en utilisant l'algorithme RSA. Le cryptogramme obtenu est C = 186.

1) Déterminer la clé secrète associée à cette clé publique.
2) Trouver le message M correspondant à ce cryptogramme.

2- Chiffre RSA :

L'algorithme RSA est utilisé pour chiffrer des données numériques. On se fixe comme nombres premiers p=29 et q=31.

1) Choisir une clé valide parmi les nombres suivants :
   Ke = 16 ; 35 ; 11 ou 21 et justifier votre choix.
2) Chiffrer la suite de messages suivante en utilisant le clé trouvée dans le 1)
   94568
3) Déterminer la clé de déchiffrement Kd associée à cette clé.

3- Chiffre Merkle-Hellman

a) Déchiffrer les cryptogrammes suivants :
   C= 149, et C = 161
   Sachant que la clé de déchiffrement est p=16, inv(p)=88, u=201 et A=(7,11,22,47,91).
b) Trouver la clé de chiffrement correspondante et chiffrer avec le message M=(1 1 1 1 1).

4- Chiffre Merkle-Hellman

L'application du chiffre de Merkle-Hellman sur un message a donné comme cryptogramme C=69. La clé utilisée est formée par :

B= (62, 93, 81, 88, 102,37) ; u= 105; p=31 et inv(p)= 61.

Trouver le message M correspondant à C.