Faculté de Technologie
Département Ingénierie des systèmes Electrique
Cryptographie et Sécurité Réseaux

Série TDN°3

Exercice 1 :

1- Effectuer les opérations suivantes :
   - M= 4^5[35], M= 4^{20}[35],
   - M= 20^3[100], M= 20^{24}[100],
   - M= 123^4[100], M= 123^{27}[100],

   NB : [35]=(mod35)
2- Calculer avec l'algorithme d'Euclide le PGCD de
   - (221,782)
   - (347,537)
   - (1755,1053)
   - (2175,3277)
3- Utiliser l'algorithme d'Euclide étendu pour déterminer un inverse de :
   - 5 modulo 16
   - 56 modulo 75.
   - 75 modulo 13

Exercice 2 :

Soit la suite super croissante suivante d={2,5,8,18,38,77}.
On prend m=149 et w=139.
-Donnez les clés privée et publique.
Ce crypto-système est utilisé pour envoyer le message suivant :
(11010001011011100011)
-Calculez le message chiffré
- Refaire le même travail pour m=158

Exercice 3:

On donne p=5 et q=11. Trouver la clé publique
Chiffrer les données M=5, M=10
Déterminer la clé privée, déchiffrer les messages chiffrés

Exercice 4 :

Le message 'elect' est chiffré à l'aide du crypto-système RSA. L'alphabet (a, b, c, ….) est codé en ASCI de 97,98,…122. Les nombres premiers du système sont p=97, q=109 et e=7.
Déterminer le message chiffré caractère par caractère

Exercice 5 :

Une banque distribue une clé publique (3, 33). On désire chiffrer le message d'un numéro de carte bancaire : 2128 2001 54 26.

- Donner le résultat de chiffrement avec la méthode RSA.
- Quelle pourrait être la clé privée. ?

Exercice 6 :

Le message 'elect' est chiffré à l'aide du crypto-système El Gamal. L'alphabet (a, b, c, ….) est codé en ASCI de 97,98,…122. Les nombres premiers du système sont p=2579. Le clé publique (g=2, p=2579, β=949), la clé du chiffreur est k=853. On donne la clé de déchiffrement :α=765

Déterminer le message chiffré caractère par caractère.