Etablissement : ENP d'Oran
Département : Génie des Systèmes
Module : Sécurité des systèmes d'information

Fiche TD 04

Exercice 01 : RSA

Bob utilise le protocole RSA et publie sa clé publique N= 85 et e=5.

1. Encoder le message m=10 avec la clé publique de Bob.
2. Supposons le message crypté x=40, retrouver le message claire m.

Exercice 02 : RSA

1. Le texte chiffré 75 a été obtenu en utilisant le RSA avec N=437 et e= 3 , vous savez que le texte en claire est soit 8 et 9 , déterminer ce nombre sans factoriser N
2. Le texte chiffré 5859 a été obtenu à l'aide du RSA en utilisant N= 11413 et e = 7467 en utilisant la factorisation suivante : 11413 = 101*113 trouver le texte clair
3. Supposons q'Alice et Bob possèdent le même nombre N utilisé dans le RSA supposons que leurs exposants respectifs e_A et e_B sont premiers entre eux
   Charles désire envoyer le message m à Alice et à Bob ; donc il le chiffre et obtient c_A et c_B . montrez q'Eve peut trouver m si elle arrive à intercepter c_A et c_B .