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 : 04

Exercice 01 :

1) En utilisant l'algorithme d'exponentiation rapide, calculez :
   $15^7 \bmod 43$ $47^{12} \bmod 17$ $35^{11} \bmod 19$
2) Calculez l'inverse dans les cas suivants :
   $7^{-1} \bmod 12$ $8^{-1} \bmod 24$ $5^{-1} \bmod 19$

Exercice 02 : Un exemple de chiffrement affine

La lettre associée à l'entier x est codée par la lettre associée à f(x), reste de la division euclidienne de 21x + 11 par 26.

1) Codez le mot RIGOLO.
2) Déterminez 21^{-1} modulo 26.
3) En déduire la fonction de décodage (à partir de la congruence $f(x) \equiv 21x + 11[26]$, trouver $x \equiv \ldots [26]$).
4) Décoder le mot GLB.

Exercice 03 : Chiffrement/Déchiffrement RSA

On considère la clef publique RSA (11, 319), c'est-à-dire pour n = 319 et e = 11.

1) Quel est le chiffrement avec cette clé du message M = 100 ?
2) Calculez d la clé privée correspondant à la clé publique e.
3) Déchiffrez le message C = 133 (sachant que $133^{25} \equiv 133 \bmod 319$).
4) Le message chiffré 625 peut-il résulter d'un chiffrement avec la clé publique ?

Exercice 04: Echange de clés Diffie-Hellman

Déterminez la clé commune d'Alice et Bob dans le cas où p = 419 et g = 7, et Alice choisit un nombre secret a = 178 et Bob choisit b = 344.