Université d'Alger1
Faculté Des Sciences
Département Mathématiques – Informatique
Module : Sécurité des systèmes d'information Licence ISIL - 2020/2021

TD3
Cryptographie Asymétrique

Exercice 1

1. Appliquer l'algorithme d'Euclide pour déterminer si les nombres 67 et 60 sont premiers entre eux.
2. Appliquer l'algorithme d'Euclide étendu pour calculer $17^{-1} \bmod 50$
3. Calculer $51447^{21} \bmod 17$

Exercice 2

On considère un module RSA n =pq, ou p et q sont les inconnus.

1. Montrer simplement comment la connaissance de ϕ(n) (la fonction d'Euler) permet de remonter à la factorisation de n.
2. Soit n =pq=84773093 un produit de deux nombres premiers. On sait que ϕ(n)= 84754668. Retrouver les deux facteurs premiers p et q de n.
3. Soit n =pq=851 un produit de deux nombres premiers. On sait que ϕ(n)=792. Retrouver les deux facteurs premiers p et q de n.

Exercice 3

Chiffrer et déchiffrer le message x dans les cas suivants (par l'algorithme de cryptage RSA)

(i) $x = 5234673$ si Bob choisit $p = 2357$, $q = 2551$ et $b = 3674911$.

(ii) $x = 9726$, si $p = 101, q = 113$

Exercice 4 (RSA)

Chiffrer le texte ITS ALL GREEK FOR ME à l'aide de petits nombres par l'algorithme de cryptage RSA. q=59, p=47.

Exercice 5

Supposant qu'Alice souhaite transmettre le message x= 1299 à Bob par l'algorithme de cryptage El-Gamal.
Sachant que : p=2579, g=2, a=765 et A=949
Décrivez le protocole d'échange en donnant le résultat de calcule de chaque étape.