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

Solution TD3
Cryptographie Asymétrique

Exercice 1

1. Déterminer si les nombres 67 et 60 sont premiers entre eux.
2. Calculer 17^{-1} mod 50

   $17^{-1} = 3 \mod 50$

3. Calcul de 51447^{21} mod 17

   $51447 = 3026 \times 17 + 5$ donc $(E) \equiv 5^{21} \mod 17$

   1. Décomposition de 21 en binaire : $21 = 2^4 + 2^2 + 2^0$
   2. Calcul de $\{5^{2^i} \mod 17\}_{0 \leq i \leq 4}$
      - $i = 0 : 5^{2^0} = 5 \mod 17$
      - $i = 1 : 5^{2^1} = 5^2 = 25 = 8 \mod 17$
      - $i = 2 : 5^{2^2} = 8^2 = 64 = 13 = -4 \mod 17$
      - $i = 3 : 5^{2^3} = (-4)^2 = 16 = -1 \mod 17$
      - $i = 4 : 5^{2^4} = (-1)^2 = 1 \mod 17$
   3. On en déduit : $5^{21} = 5^{2^4} \times 5^{2^2} \times 5^{2^0} = 1 \times (-4) \times 5 = -20 = 14 \mod 17$

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.

Solution pour les questions 1 et 2:

Rappelons que dans le fonctionnement de RSA, la connaissance de $\varphi(n)$ suffit au cryptanalyste pour calculer l'exposant de déchiffrement ou pour factoriser n. Dans ce cas il peut écrire les équations $n = pq$ et $\varphi(n) = (p-1)(q-1)$ et en déduire la seule équation du second degré en éliminant $q = n/p$.

$$p^2 - (n - \varphi(n) + 1)p + n = 0$$

Donc on a :

$p^2 - 18426p + 84773093 = 0$. Les solutions $p = 9539$ et $q = 8887$ Sont justement la factorisation de n.

Exercice 3

Chiffrer et déchiffrer le message x dans les cas suivants (en utilisant RSA)

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

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

Solution :

(ii) $n = pq = 11413$, et $\varphi(n) = 100 \times 112 = 11200$. Comme $11200 = 2^6 \times 5^2 \times 7$, un entier b peut être utilisé comme exposant de chiffrement si et seulement si n'est pas divisible 2, 5 et 7. Si Bob choisit $b = 3533$, il obtient à l'aide de l'algorithme d'Euclide $b^{-1} = 6597 \bmod 11200$. et par conséquent, l'algorithme de déchiffrement . Bob publie sa clé publique dans un répertoire $(n,b) = (11413, 3533)$. Pour transmettre le message $x = 9726$ à Bob, Alice calcule $9726^{3533} \bmod 11413 = 5761$; Bob n'a qu'à calculer $5761^{6597} \bmod 11413 = 9726$.

Exercice 4

Chiffrer le texte ITS ALL GREEK FOR ME à l'aide de petits nombres q=59,p=47 (en utilisant RSA)

Solution : Modifions un peu l'alphabet en codant Espace=0, A=1, B=2,…,Z=26 . Par conséquent $M = C = Z_{27}$. On peut penser à coder le message par blocs

$x = 0920 \quad 1900 \quad 0112 \quad 1200 \quad 0718 \quad 0505 \quad 1100 \quad 2015$

$0013 \quad 0500$

$n = pq = 2773$, $\varphi(n) = (p-1)(q-1) = 2668$; l'exposant de chiffrement doit être « grand » et premier avec $2668 = 2^2 \times 23 \times 29$; ici nous prenons $b = 17$; la clé publique est $(n,b) = (2773,17)$; La clé privée est $a = b^{-1} \bmod 2773 =$

Le premier bloc $x_1 = 0920$ donne $y_1 = 920^{17} = 948 \bmod 2773$ etc…
On obtient,

$y = 0948 \;\; 2342 \;\; 1084 \;\; 1444 \;\; 2663 \;\; 2390 \;\; 0778 \;\; 0774 \;\; 0919 \;\; 1655$

Pour déchiffrer, on calcule $948^{157} \bmod 2773 = 920$, soit 09 20 qui est le code de IT etc….

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.

Solution :

Supposons que $p := 2579$, $g := 2, a = 765$, alors $A = 2^{765} \bmod 2579 = 949$. Si l'émetteur (Alice) souhaite transmettre le message $x = 1299$ à Bob, il commence à choisir au hasard m, disons $m = 853$. Il calcule ensuite $y_1 = 2^{853} \bmod 2579 = 435$; puis $y_2 = 1299 \times 949^{853} \bmod 2579 = 2396$. Lorsque Bob reçoit le texte chiffré $y = (435,2396)$, il calcule

$x = 2396 \times \left(435^{765}\right)^{-1} \bmod 2579 = 1299$ qui est bien le texte clair.