TD 2 : Le cryptosystème RSA

Exercice 1

On utilise les notations habituelles du RSA : p,q, n, ϕ(n), e et d

1. Donner les formules qui définissent les variables n, ϕ(n) et d en fonction d'une ou de plusieurs autres variables.

2. On chiffre un message m qui devient le message c en utilisant l'algorithme de chiffrement asymétrique RSA

   a. Quelle est la formule de chiffrement ?
   b. Quelle est la formule de déchiffrement ?
   c. Quelles sont les valeurs qui doivent rester secrètes parmi n, p, q, ϕ(n), e, d ?
   d. Quelles sont les valeurs publiques parmi n, p, q, ϕ(n), e, d ?

3. En appliquant l'algorithme étendu d'Euclid, calculer **d** pour p=61, q=137 et e=7.
4. Chiffrez le Message M = "Bonjour GL".

Exercice 2

On considère les valeurs p = 53, q = 11 et e = 3.

a) Calculez la valeur publique n.
b) Calculez la fonction d'Euler ϕ(n) = (p − 1)(q − 1).
c) Utilisez l'algorithme étendu d'Euclid pour calculer la valeur **d** de la clé privée.
   1. Donnez la clé publique.
   2. Donnez la clé secrète..
d) Chiffrez le Message M = "**Salut GL**".

Exercice 3: Cryptage ElGamal

On considère les valeurs p = 97, g = 13 et, a = 45 choisies par Alice, la valeur b=76 choisie par Bob.

a) Rappelez l'algorithme de cryptage ElGamal.
b) Donnez la clé publique.
c) Donnez la clé secrète.
d) Chiffrez le Message M = "Salut GL".

Exercice 1

3. En appliquant l'algorithme étendu d'Euclid, calculer **d** pour p=61, q=137 et e=7.

soit p=61, q=137 et e=7
$n = p \times q = 8357$
$\varphi(n) = (p - 1) \times (q - 1) = 8160$

$d = ?$

Algorithme étendu d'Euclid

Q	A	B	R	T1	T2	T
1165	8160	7	5	0	1	-1165
1	7	5	2	1	-1165	1166
2	5	2	1	-1165	1166	-3497
2	2	1	0	1166	-3497	8160

T2 < 0 donc d = $\varphi(n)$ + (T2) = 8160 -3497 = 4663
donc d = 4663

4. Chiffrez le Message M = "Bonjour GL".

- Pour crypter un message M < n, l'émetteur:
  - ✓ Obtient une clé publique du récepteur et calcule « $C = M^e \bmod n$ »
- Pour décrypter un message crypté C le récepteur
  - ✓ Utilise sa clé privée et calcule « $M = C^d \bmod n$ »

code **ASCII** ⇒ Bonjour GL ⇒ 66,111,110,106,111,117,114,32,71,76

66 111 110 106 111 117 114 32 71 76

$C_{66} = 66^7 \bmod 8357 = 2546$
$C_{111} = 111^7 \bmod 8357 = 3610$
etc …

etc…

le message crypté = **2546, 3610, 8071, 5780, 3610, 5933, 6372, 8081, 331, 6976**

Exercice 3

a)

b)

La clé publique (p, g, α)

- $\alpha = (g^a \bmod p) = 13^{45} \bmod 97 = 20$

donc la clé publique (97, 13, 10)

c) la clé secrète

a = 45

d)

pour Chiffrer le Message M = “Salut GL”

passage vers code ascii 83 97 108 117 116 32 71 76 l'exprime sous la forme d'un nombre entre 0 et p-1 avec p = 97 donc 83 9 71 08 11 71 16 32 71 76

avec $m' = \alpha^b \bullet m \bmod p$

Donc

C_{83} **=** 20^76 * 83 mod 97 = **23**
C_9 **= 20^76 * 9 mod 97** = 6
C_{71} **= 20^76 *** 71 **mod 97** = 15
etc …

donc le message crypté est: 23 6 15 **70 72 15 43 86 15 83**