**Exercice 2 :** (RSA)Soit p = 7 et q= 19
- Calculer n et Ф (n).
- On propose e = 5. Calculer la clé privée d.
- Chiffrer le message clair m =6.
- Déchiffrer le message chiffré c= 62.

**Solution :**

Le schéma suivant récapitule le principe du chiffrement RSA :

****

* **Calculer n et Ф (n).**

**n= p × q** = 7 × 19 = 133

**Ф (n)= (p-1) (q-1)=** 6 × 18 = 108

* **On propose e = 5. Calculer la clé privée d**

On a **d × e = 1 𝑚𝑜𝑑 (Ф (n))** donc on calcule d par l’algorithme d’Euclide étendu :

e = 5 et on a bien pgcd (e, Ф (n)) = pgcd(5,108)=1 donc la clé privée d= 65

* **Chiffrer le message clair m =6.**

Le message chiffré se calcule x ≡ m𝑒 𝑚𝑜𝑑 𝑛. On a m= 6, N= 133 et e= 5 donc :

x ≡ m𝑒 𝑚𝑜𝑑 𝑛 ≡ 65 𝑚𝑜𝑑 133 ≡ 62 𝑚𝑜𝑑 133

Le message chiffré est donc : 62

* **Déchiffrer le message chiffré c= 62.**

Le déchiffrement se fait grâce au calcul m ≡ x𝑑 𝑚𝑜𝑑 𝑛

On a x = 62, d=65 et N = 133 donc m = x𝑑 𝑚𝑜𝑑 𝑛 ≡ 6265 𝑚𝑜𝑑 133 ≡ 6 𝑚𝑜𝑑 133

Le message clair est donc : m= 6

**Exercice 3 :** *(RSA)*- Déchiffrer le message reçu 18 chiffré avec la clé publique (35;11).
- Chiffrer le message M = 10 avec la clé publique (55;7). Calculer p; q et d. Déchiffrer C = 35.

**Solution :**

* **Déchiffrer le message reçu 18 chiffré avec la clé publique (35;11).**

On a : 𝑛 = 35 = 5 × 7 ⟹ 𝑝 = 5 𝑒𝑡 𝑞 = 7

Ф (n) = (𝑝 – 1) (𝑞 – 1) = 4 × 6 = 24
e = 11 pour trouver d on a: e × d = 1 𝑚𝑜𝑑 24, d = e-1 𝑚𝑜𝑑 24 = 11-1𝑚𝑜𝑑 24

Donc 𝑑 = 11 𝑚𝑜𝑑 24 (car 11 × 11= 1 𝑚𝑜𝑑 24)

On déchiffre x =18 par le calcul suivant :

 m = xd 𝑚𝑜𝑑 𝑛 = 1811 𝑚𝑜𝑑 35 = 2 𝑚𝑜𝑑 35

Donc le message clair est m = 𝟐

* **Chiffrer le message m=10 avec la clé publique (55, 7)**

On a : e=7 et n= 55 donc x = m𝑒 𝑚𝑜𝑑 𝑛 = 107𝑚𝑜𝑑 55 = 10 𝑚𝑜𝑑 55

Donc le message chiffré est x = 𝟏𝟎

* **Calculer p; q et d.**

𝑛 = 55 = 5 × 11 ⟹ 𝒑 = 𝟓 𝑒𝑡 𝒒 = 𝟏𝟏

Ф (n) = (𝑝 – 1) (𝑞 – 1) = 4 × 10 = **40**

e = 7 pour trouver d on a: e × d = 1 𝑚𝑜𝑑 40, d = e-1 𝑚𝑜𝑑 40 = 7-1𝑚𝑜𝑑 40

Donc 𝒅 = -𝟏𝟕 𝒎𝒐𝒅 𝟒𝟎 = 𝟐𝟑 𝒎𝒐𝒅 𝟒𝟎

Donc p= 𝟓, q = 𝟏𝟏 et d=**23**

* **Déchiffrer C = 35**

On déchiffre x =35 par le calcul suivant :

m = x𝑑 𝑚𝑜𝑑 𝑛 = 3523 𝑚𝑜𝑑 55 = 30

Le message clair est donc : m= **30**

**Exercice 4 :** *(EL GAMAL)*Prenons p = 2357 et g = 2 qui est d'ordre maximal 2356.
- Bob choisit a = 1751; calculer la valeur de b.
- Déduire la clé publique et la clé privée.
- Si Alice choisit k = 1520, chiffrer le message m = 2035.

**Solution :**

**- Bob choisit a = 1751; calculer la valeur de b.**

On a b= **ga 𝑚𝑜𝑑** **p** =21751mod 2357donc b=1185

**- Déduire la clé publique et la clé privée.**

La clé publique est b=1185 et la clé privée est a=1751

**- Si Alice choisit k = 1520, chiffrer le message m = 2035.**

Si Alice a choisi k=1520 donc pour calculer le message chiffré on a **c=m bk 𝑚𝑜𝑑 p**

c=2035 × 11851520 𝑚𝑜𝑑 2357=2035 × 2084 𝑚𝑜𝑑 2357=697 𝑚𝑜𝑑 2357

Donc le massage chiffré est c=697

Ce tableau récapitule la solution de l’exercice avec une question supplémentaire sur le déchiffrement.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Alice | Les deux | Bob |
| Connaît | k = 1520 | p = 2357, g = 2 | a = 1751 |
| Calcule | l=**gk mod p**l=21520 mod 2357l=1430 |  | b= **ga mod p**b=21751mod 2357b=1185 |
| Clé publique | l=1430 | l,b | b=1185 |
| Clé privée | k = 1520 |  | a =1751 |
| Chiffrement  | m = 2035c=m **bk mod p**c=2035 × 11851520 mod 2357c=2035 × 2084 mod 2357c=697 | c=697 |  |
| Déchiffrement  |  | c=697, m=2035 | c=697c=m **la mod p**697=m ×14301751mod 2357697=m × 2084 mod 2357m= 2084-1 × 697 mod 2357m= 872 × 697 mod 2357m=2035 |