Solution TD 5

Exercice 1

1- Pour montrer que le couple (35,5) est une clé publique valide pour RSA, nous devons vérifier deux conditions :

- La clé publique doit être composée de deux nombres premiers distincts :

  Dans ce cas, nous avons deux nombres premiers distincts, qui sont 5 et 7. La clé publique est donc valide selon cette condition.

- Le nombre 5 doit être premier par rapport à l'indice d'Euler de n :

  L'indice d'Euler de n est défini comme suit : φ(n) = (p-1) (q-1), où **p** et **q** sont les deux nombres premiers utilisés pour construire la clé publique.

  Dans notre cas, p = 5 et q = 7, donc n = p× q = 35 et φ(n) = (5-1) (7-1) = 24.

  Pour vérifier que 5 est premier par rapport à 24, nous devons trouver le plus grand diviseur commun entre 5 et 24. Nous pouvons utiliser l'algorithme d'Euclide pour cela :

  24 = 5×4 + 4

  5 = 4×1 + 1

  Le plus grand diviseur commun est donc 1. Comme 5 et 24 sont premiers entre eux, la clé publique est valide selon cette condition. Ainsi, le couple (35,5) est une clé publique valide pour RSA.

2- Calculer la clé privée d :

$$n = 35\,, e = 5\,, \varphi(\mathrm{n}) = 24$$

$$d.e = 1 \; mod \; \varphi(\mathrm{n}) \qquad\qquad \mathrm{PGCD}(5.24) = 1$$

Pour résoudre cette équation, nous pouvons utiliser l'algorithme d'inversion modulo. On cherche donc l'entier d tel que $\underline{5} \times \mathbf{d} \equiv 1 \pmod{24}$.

$1 = 5 - 4 \times 1$

$1 = 5 - (24 - 5 \times 1)$

$1 = 5 - 24 + 5 \times 4$

$1 = -24 + \underline{5} \times \mathbf{5}$

La clé privée est $\boldsymbol{d} = \mathbf{5}$

3- Chiffrement le message **m = code :**

a- Pour chiffrer le mot (code) en RSA, nous devons d'abord convertir chaque lettre (ou caractère) en un entier correspondant à le tableau :

C = 3, O = 19 , D = 4 , E = 5 ➔ Code ➔ [03,19,04,05]

Ensuite, nous utilisons la clé publique (n, e) = (35, 5) pour chiffrer le message. Pour cela, nous chiffrons chaque entier séparément en utilisant la formule suivante : $\boldsymbol{c = m^e\, mod(n)}$

Pour le **premier** entier, **03**, nous avons :

$c_1 = 3^1\ mod\ 35 = \mathbf{3}$

$c_1 = 3^2\ mod\ 35 = \mathbf{9}$

$c_1 = 3^4\ mod\ 35 = \mathbf{11}$

$c_1 = 3^5\ mod\ 35 = (\mathbf{11} \times \mathbf{3})\boldsymbol{mod}\ \mathbf{35}$

$\boldsymbol{c_1} = \mathbf{33}$

Pour le **deuxième** entier, **19**, nous avons :

$c_2 = 19^1\ mod\ 35 = \mathbf{19}$

$c_2 = 19^2\ mod\ 35 = \mathbf{11}$

$c_2 = 19^4\ mod\ 35 = \mathbf{16}$

$c_2 = 19^5\ mod\ 35 = (\mathbf{19} \times \mathbf{16})\boldsymbol{mod}\ \mathbf{35}$

$\boldsymbol{c_2} = \mathbf{24}$

Pour le **troisième** entier, **04**, nous avons :

$c_3 = 4^1\ mod\ 35 = \mathbf{4}$

$c_3 = 4^2\ mod\ 35 = \mathbf{16}$

$c_3 = 4^4\ mod\ 35 = \mathbf{11}$

$c_3 = 4^5\ mod\ 35 = (\mathbf{4} \times \mathbf{11})\boldsymbol{mod}\ \mathbf{35}$

$\boldsymbol{c_3} = \mathbf{09}$

Pour le **quatrième** entier,**05**, nous avons :

$c_4 = 5^1\ mod\ 35 = \mathbf{5}$

$c_4 = 5^2\ mod\ 35 = \mathbf{25}$

$c_4 = 5^4\ mod\ 35 = \mathbf{30}$

$c_4 = 5^5\ mod\ 35 = (\mathbf{5} \times \mathbf{30})\boldsymbol{mod}\ \mathbf{35}$

$\boldsymbol{c_4} = \mathbf{10}$

Ainsi, notre message chiffré sera représenté par la séquence d'entiers **C** = [**33, 34,09, 10]** ➔ **(FYXS).**

b- Déchiffrement le message C :

La clé privée (n, d) = (35, 5), nous pouvons déchiffrer le message chiffré en utilisant la formule suivante : $\boldsymbol{m = c^d\, mod(n)}$

Pour le **premier** entier,**33**, nous avons :

$m_1 = 33^1\ mod\ 35 = \mathbf{33}$

$m_1 = 33^2\ mod\ 35 = \mathbf{4}$

$m_1 = 33^4\ mod\ 35 = \mathbf{16}$

$m_1 = 33^5\ mod\ 35 = (\mathbf{33} \times \mathbf{16})\boldsymbol{mod}\ \mathbf{35}$

$\boldsymbol{m_1} = \mathbf{03}$

Pour le **deuxième** entier, **24**, nous avons :

$m_2 = 24^1\ mod\ 35 = \mathbf{24}$

$m_2 = 24^2\ mod\ 35 = \mathbf{16}$

$m_2 = 24^4\ mod\ 35 = \mathbf{11}$

$m_2 = 24^5\ mod\ 35 = (\mathbf{24} \times \mathbf{11})\boldsymbol{mod}\ \mathbf{35}$

$\boldsymbol{m_2} = \mathbf{19}$

Pour le **troisième** entier, **09**, nous avons :

$m_3 = 9^1\ mod\ 35 = \mathbf{9}$

$m_3 = 9^2\ mod\ 35 = \mathbf{11}$

$m_3 = 9^4\ mod\ 35 = \mathbf{16}$

$m_3 = 9^5\ mod\ 35 = (\mathbf{16} \times \mathbf{9})\boldsymbol{mod}\ \mathbf{35}$

$\boldsymbol{m_3} = \mathbf{04}$

Pour le **quatrième** entier, **10**, nous avons :

$m_4 = 10^1\ mod\ 35 = \mathbf{10}$

$m_4 = 10^2\ mod\ 35 = \mathbf{30}$

$m_4 = 10^4\ mod\ 35 = \mathbf{25}$

$m_4 = 10^5\ mod\ 35 = (\mathbf{10} \times \mathbf{25})\boldsymbol{mod}\ \mathbf{35}$

$\boldsymbol{m_4} = \mathbf{05}$

Ainsi, notre message clair sera représenté par la séquence d'entiers **M** = [**03, 19,04, 05]** ➔ **(CODE).**

Exercice 2 :

a- La clé privée :

$$\varphi(n) = 840 \; et \; e = 13$$

$d \times \mathrm{e} = 1\mathrm{mod}\ \varphi(\mathrm{n})$ $\mathrm{PGCD}(13.840) = 1$

Pour résoudre cette équation, nous pouvons utiliser l'algorithme d'inversion modulo. On cherche donc l'entier d tel que $13 \times \mathbf{d} \equiv 1 \ (\mathrm{mod}\ 840)$.

$840 = 13 \times 64 + 08$

$13 = 08 \times 01 + 05$

$08 = 05 \times 01 + 03$

$05 = 03 \times 01 + 02$

$03 = 02 \times 01 + \mathbf{01}$

$1 = 3 - 2$

$1 = 3 - (5 - 3)$

$1 = 3 - 5 + 3$

$1 = 2 \times (8 - 5) - 5$

$1 = 2 \times 8 - 5 \times 3$

$1 = 2 \times 8 - 3 \times (13 - 8)$

$1 = 2 \times 8 - 3 \times 13 + 8 \times 3$

$1 = 5 \times 8 - 3 \times 13$

$1 = 5 \times (840 - 13 \times 64) - 13 \times 3$

$1 = 5 \times 840 + 13 \times (\mathbf{-323})$

$-323 < 0$ ➔ $840 - 323 = 517$

La clé privée est $\boldsymbol{d} = \mathbf{517}$

b- Déchiffrement le message $\boldsymbol{c} = \mathbf{676141}$

$\mathrm{m} = \mathrm{c}^{\mathrm{d}}\mathrm{mod}(\mathrm{n})$

$\mathrm{n} = 899$

$d = 517$

La clé privée (n, d) = (899, 517), nous pouvons déchiffrer le message chiffré en utilisant la formule suivante : $\boldsymbol{m = c^d\, mod(n)}$

Pour le **premier** entier,**676**, nous avons :

$m_1 = 676^1\ mod\ 899 = \mathbf{676}$

$m_1 = 676^2\ mod\ 899 = 284$

$m_1 = 676^4\ mod\ 899 = \mathbf{645}$

$m_1 = 676^8\ mod\ 899 = 687$

$m_1 = 676^{16}\ mod\ 899 = 893$

$m_1 = 676^{32}\ mod\ 899 = 36$

$m_1 = 676^{64}\ mod\ 899 = 397$

$m_1 = 676^{128}\ mod\ 899 = 284$

$m_1 = 676^{256}\ mod\ 899 = 645$

$m_1 = 676^{512}\ mod\ 899 = \mathbf{687}$

$\boldsymbol{m_1} = 676^{517} mod 899 = (676 \times 645 \times 687) mod\ 899$

$\boldsymbol{m_1} = 738$

Pour le **deuxième** entier, **141**, nous avons :

$m_2 = 141^1\ mod\ 899 = \mathbf{141}$

$m_2 = 141^2\ mod\ 899 = 103$

$m_2 = 141^4\ mod\ 899 = \mathbf{720}$

$m_2 = 141^8\ mod\ 899 = 576$

$m_2 = 141^{16}\ mod\ 899 = 45$

$m_2 = 141^{32}\ mod\ 899 = 227$

$m_2 = 141^{64}\ mod\ 899 = 286$

$m_2 = 141^{128}\ mod\ 899 = 886$

$m_2 = 141^{256}\ mod\ 899 = 169$

$m_2 = 141^{512}\ mod\ 899 = \mathbf{692}$

$\boldsymbol{m_2} = 141^{517}\ mod\ 899 = (141 \times 720 \times 692) mod\ 899$

$\boldsymbol{m_2} = 384$

Ainsi, notre message clair sera représenté par la séquence d'entiers $\mathrm{M} = 738384$