TD Cryptographie

ENSSAT

Exercice 5

1. Remarquons que $24 = 3 \times 2^3$. Puisque 3 et 2 sont premiers entre eux, on a
$$\begin{aligned}\varphi(24) &= \varphi(3)\varphi(2^3) \\ &= (3-1)(2^3-2^2) = 8\end{aligned}$$
2. Les inversibles de $\mathbb{Z}/24\mathbb{Z}$ sont les nombres entiers premiers avec 24. Il y a
$$\{1,5,7,11,13,17,19,23\}$$
et il y en a bien 8.
5 est inversible car premier avec 24 et son inverse est lui-même : $\overline{5} \times \overline{5} = \overline{25} = \overline{1}$ dans $\mathbb{Z}/24\mathbb{Z}$.
3. 5 est un générateur de $(Z/24\mathbb{Z}, +)$ car inversible dans $(\mathbb{Z}/24\mathbb{Z}, \times)$. Par addition modulo 24 successives :
$$\{5,10,15,20,1,6,11,16,21,2,7,12,17,22,3,8,13,18,23,4,9,14,19,0\}$$

Exercice 6

1. Notons c l'inverse de a modulo n. Alors :
$$\begin{aligned}ax+b = y \mod n &\iff ax = y-b \mod n \\ &\iff x = c(y-b) \mod n\end{aligned}$$
Ainsi, la règle de déchiffrement d_k vérifie :
$$d_k(y) = c(y-b) \mod n$$
On ne peut cependant pas choisir n'importe quelle clé. En effet, si a n'est pas inversible modulo n, alors on ne peut pas inverser. Il est donc nécessaire, et suffisant, d'avoir a inversible modulo n, c'est-à-dire a premier avec n.
2. Prenons $a = 5$ et $b = 2$. PGCD$(5,26) = 1$ et le couple (a,b) est une bonne clé. Alors la clé de décryptage est
$$d_k(y) = 21(y-2) \mod 26 = 21y + 10 \mod 26$$
3. Par définition, il y a $\varphi(n)$ éléments premiers de $\mathbb{Z}_n$ premier avec n, et il y a donc $n \times \varphi(n)$ clés possibles : n choix pour b, $\varphi(n)$ pour a. Dans tous les cas, il y a en moins de n^2 et est donc facilement déchiffrable en testant toutes les clés possibles.

Exercice 7

1. Alice doit envoyer $x^b \mod n$, c'est-à-dire $12^{17} \mod 35$, que l'on calcule par la méthode que l'on souhaite, par exemple l'exponentiation rapide :
$$12^2 \equiv 4 \mod n \text{ donc } 12^4 \equiv 4^2 = 16 \mod n \text{ et } 12^8 \equiv 16^2 \equiv 11 \mod n$$
mais alors
$$12^{17} = 12^8 12^8 12 \equiv 11 \times 11 \times 12 \equiv 17 \mod n$$
Ainsi, Alice envoie le message crypté 17.

2. Bob a choisi comme clé publique $b = 17$ et $n = 35$. Remarquons que

$$\varphi(35) = \varphi(5 \times 7) = \varphi(7)\varphi(5) = 6 \times 4 = 24$$

donc 17 est bien premier avec $\varphi(n)$. On doit chercher l'inverse de 17 modulo $\varphi(n) = 24$. Pour cela, on détermine par l'algorithme d'Euclide étendu le PGCD de 17 et 24 (qui vaut 1). En remontant, on obtiendra

$$5 \times 24 - 7 \times 17 = 1 =$$

et donc, modulo 24, -7 est l'inverse, c'est-à-dire aussi $-7 + 24 = 17$ (on prend l'entier positif entre 1 et 24. Donc $e = 17$ est l'inverse de 17.
Il suffit alors à Oscar de calculer message$^e \mod n$ pour déterminer le message originel. Ainsi il faut calculer $17^{17} \mod 35$. Or :

$$17^2 \equiv 9 \mod 35 \quad \text{puis} \quad 17^4 \equiv 9^2 \equiv 11 \mod 35 \quad ,17^8 \equiv 16 \mod 35 \quad \text{et} \quad 17^{16} \equiv 16^2 \equiv 11 \mod 35$$

et alors

$$17^{17} = 17^{16} \times 17 \equiv 11 \times 17 \equiv 12 \mod 35$$

On retrouve bien le message décrypté originel.

Exercice 8

Il suffit à Oscar de calculer $y_1^u y_2^v \mod n$. En effet :

$$\begin{aligned} y_1^u y_2^v &\equiv x^{a_1 u} x^{a_2 v} \mod n \\ &\equiv x^{a_1 u + a_2 v} \mod n \\ &\equiv x \mod n \end{aligned}$$

Le problème, puisque $u \leqslant 0$ est de calculer $y_1^u \mod n$. Or, par hypothèse, y_1 est premier avec n. Par l'algorithme d'Euclide étendu, on déterminer z_1 l'inverse de y_1 modulo n. Alors

$$y_1^u \equiv z_1^{-u} \mod n$$

et cette fois-ci, $-u \geqslant 0$ et se calcule habituellement.

Exercice 9

Le théorème chinois

1. Par définition, $m_i' = m_1 \dots m_{i-1} m_{i+1} \dots m_k$ qui est donc le produit de $k-1$ nombres premiers avec m_i : m_i' est donc bien un entier premier avec m_i.
2. m_i' étant premier avec m_i, il est inversible dans $\mathbb{Z}_{m_i}$. On obtient son inverse en appliquant l'algorithme d'Euclide étendu à m_i et m_i'.
3. (a) Par définition, m_j'' est l'inverse m_j' modulo m_j donc

$$m_j' m_j'' \equiv 1 \mod m_j \quad \text{et} \quad a_j m_j' m_j'' \equiv a_j \mod m_j$$

   (b) Par définition, m_j apparait dans l'entier m_i' si $i \neq j$, donc $m' i \equiv 0 \mod m_j$ et donc $a_i m_i' m_i'' \equiv 0 \mod m_j$.

(c) Ainsi, on a

$$\sum_{i=1}^{k} a_i m_i' m_i'' \equiv a_j \mod m_j$$

en utilisant les deux résultats précédents (pour $i = j$ et pour $i \neq j$. Donc, pour tout j, $x \equiv a_j \mod m_j$: x est bien solution de (2) dans $\mathbb{Z}_m$ (il est bien dans $\mathbb{Z}_m$ car on a pris la somme modulo m).

4. D'après la question précédente, soit $(a_1, \cdots, a_k) \in \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ quelconque. On peut trouver $x \in \mathbb{Z}_m$ solution de (2). Mais alors $f(x) = (a_1, \cdots, a_k)$ et f est bien surjective.
De plus, le cardinal de $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_k}$ est égal à $m_1 \times \cdots \times m_k = m$ qui est le cardinal de $\mathbb{Z}_m$. Ainsi, f est une application surjective sur des espaces de même cardinal : elle est bijective.
Puisqu'elle est bijective, elle est injective et pour tout $(a_1, , \cdots, a_k) \in \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ il existe une unique solution x vérifiant $f(x) = (a_1, \cdots, a_k)$.

Application

1. Concrètement, en utilisant les notations de la partie précédente, Oscar dispose de $x^3 \mod n_1, x^3 \mod n_2, x^3 \mod n_3$, avec n_1, n_2, n_3 deux à deux premiers entre eux. La question 4 précédente garantie qu'il existe une unique solution $y = x^3 \in \mathbb{Z}_m$ (où $m = n_1 n_2 n_3$) vérifiant $f(x) = (y_1, y_2, y_3)$. x est alors le message envoyé par Alice.
En pratique, Oscar calcule (par l'algorithme d'Euclide étendu) l'inverse de n_1', n_2' et n_3' et calcule y par la formule (3).
Or y représente $x^3 \mod m$ (x étant le message cherché). Mais par définition de RSA, $x < n_1, x < n_2$ et $x < n_3$ donc $x^3 < n_1 n_2 n_3 = m$. Donc $x^3 \mod m = x^3$ et il suffit de calculer $x = y^{1/3}$ (racine cubique classique).
2. Concrètement, pour pouvoir calculer x aussi efficacement, il faut appliquer le théorème chinois (ce qui va relativement vite, avec Euclide étendu) mais aussi résoudre $y = x^d \mod m$ d'inconnue y. Le plus efficace est de connaitre d valeurs (même message envoyé à d personnes) : ainsi, il suffit de calculer la racine d-ième du nombre obtenu.