TD Cryptographie

ENSSAT

Exercice 1

Exercice 2

1. Si l'équation (1) admet au moins une solution, il existe $(x, y) \in \mathbb{Z}^2$ tels que

$$ax + by = c$$

Notons $d = \text{PGCD}(a, b)$. d divise a et b, donc divise $ax + by$, c'est-à-dire que d divise c.

2. Réciproquement, si c divise d, et quitte à diviser par d, on obtient l'équation

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$$

où $a' = \frac{a}{d}, b' = \frac{b}{d}$ et $c' = \frac{c}{d}$ sont des entiers. Par définition du PGCD :

$$\text{PGCD}(a, b) = \text{PGCD}\left(da', db'\right) = d\text{PGCD}(a', b')$$

et donc $\text{PGCD}(a', b') = 1$. Ainsi, on peut supposer que a et b sont premiers entre eux, quitte à diviser l'équation par le PGCD de a et b.
On peut alors obtenir un couple (u, v) vérifiant $au + bv = 1$ (par l'algorithme d'Eculide), et alors

$$a(cu) + b(cv) = c$$

et le coupe (cu, cv) est solution de (1).
Connaissant une solution particulière de (1), qu'on note (x_0, y_0), on en déduit, par soustraction, que (x, y) vérifie (1) si et seulement si

$$a(x - x_0) = b(y_0 - y)$$

Puisqu'on a supposé a et b premiers entre eux, cela indique que a divise $y_0 - y$ (théorème de Gauss) et donc que $y = y_0 - ka$ avec $k \in \mathbb{Z}$. En injectant dans l'équation précédente, on a alors

$$a(x - x_0) = bka \Leftrightarrow x = x_0 + kb$$

Ainsi l'ensemble des solutions est de (1) est

$$\mathscr{S} = \left\{(x_0 - ka, y_0 + kb), \quad k \in \mathbb{Z}\right\}$$

3. Remarquons que $\text{PGCD}(15, 6) = 3$. Ainsi

$$15x - 6y = 9 \Leftrightarrow 5x - 2y = 3$$

5 et 2 sont premiers entre eux. On applique l'algorithme d'Euclide étendue pour une obtenir une solution, ou alors on constate que $(1, 1)$ est une solution particulière évidente. Alors, par soustraction

$$5x - 2y = 3 \Leftrightarrow 5(x - 1) - 2(y - 1) = 0 \Leftrightarrow 5(x - 1) = 2(y - 1)$$

5 et 2 sont premiers entre eux. D'après le théorème de Gauss, on en déduit que 5 divise $y - 1$ et donc qu'il existe $k \in \mathbb{Z}$ tel que $y - 1 = 5k$, c'est-à-dire $y = 1 + 5k$. En injectant dans l'équation précédente, on obtient

$$5(x - 1) = 2 \times 5k \Leftrightarrow x = 1 + 2k$$

Ainsi, l'ensemble des solutions est

$$\mathscr{S} = \{(1 + 2k, 1 + 5k), \quad k \in \mathbb{Z}\}$$

Exercice 3

Remarquons que, en majorant grossièrement :

$$4444^{4444} < 10000^{4444} = 10^{17776}$$

Donc 4444^{4444} possède moins de 17776 chiffres. Donc

$$\begin{aligned} f\left(4444^{4444}\right) &\leqslant f(999\cdots999) = 17776 \times 9 < 160000 \\ \text{puis } f \circ f\left(4444^{4444}\right) &\leqslant f(999999) = 54 \\ \text{et } f \circ f \circ f\left(4444^{4444}\right) &< f(59) = 5+9 = 14 \end{aligned}$$

On doit donc trouver un moyen de trouver l'entier entre 1 et 13 qui est égal $f \circ f \circ f(\mathrm{N})$. Utilisons une propriété usuelle de la division par 9 : un nombre N est congrus à sa somme de chiffre modulo 9. Ainsi

$$f(\mathrm{N}) \equiv f \circ f(\mathrm{N}) \equiv f \circ f \circ f(\mathrm{N}) \equiv \mathrm{N} \mod 9$$

Or $4444 \equiv 7 \mod 9$, donc $4444^3 \equiv 1 \mod 9$. Ainsi

$$4444^{4444} = 4444^{1481\times3} \times 4444 \equiv 1^{1481} \times 7 = 7 \mod 9$$

Ainsi $f \circ f \circ f(\mathrm{N}) \equiv 7 \mod 9$.

Le seul nombre entier congru à 7 modulo 9 dans l'intervalle $[\![1;13]\!]$ étant 7, on en déduit donc que

$$f \circ f \circ f(\mathrm{N}) = 7$$

Exercice 4

Généralités

1. En utilisant les notation du cours, on a l'invariant de boucle :

$$\begin{cases} u_0 a + v_0 b &= r_0 \\ u_1 a + v_1 b &= r_1 \\ r_1 &\geqslant 0 \end{cases}$$

2.

Analyse de l'algorithme d'Euclide

1. (a) D'après l'algorithme d'Euclide, on a, pour $1 \leqslant i \leqslant \mathrm{N}_1$: :

$$r_{i-2} = q_i r_{i-1} + r_i$$

(b)

2. (a) Pour $k = N-1$, alors $\varphi^{N-1-k} = 1$ et on a, par construction, $r_{N-1} \geqslant 1$ (et $r_N = 0$ premier reste nul). Par hérédité, supposons que pour tout $n \leqslant k \leqslant N-1$, $r_k \geqslant \varphi^{N-1-k}$. Montrons que le résultat est vrai pour r_{k-1} :

$$\begin{aligned} r_{k-1} &= q_{k+1} r_k + r_{k+1} \\ &\geqslant q_{k+1} \varphi^{N-1-k} + \varphi^{N-1-(k+1)} \\ &\geqslant \varphi^{N-k-2} \left(\varphi + 1\right) \\ &\geqslant \varphi^{N-k-2)} \varphi^2 \text{ car } \varphi^2 = \varphi + 1 \\ &\geqslant \varphi^{N-k} = \varphi^{(N-1)-(k-1)} \end{aligned}$$

Par récurrence descendante, on a donc bien le résultat.

(b) Puisque $r_0 = b$, on a alors :

$$\begin{aligned} r_0 = b \Rightarrow & \qquad\qquad b \geqslant \varphi^{N_1} \\ \Rightarrow & \ln(b) \geqslant (N-1)\ln(\varphi) \\ \Rightarrow & N \leqslant \log_\varphi(b) + 1 \text{ où } \log_\varphi(b) = \frac{\ln(b)}{\ln(\varphi)} \text{ (car } \ln(\varphi) > 0) \end{aligned}$$

(c) L'algorithme est assez efficace. Par exemple, pour N = 100000, on a $N \leqslant 30$.

(d) Pour Euclide étendu, c'est aussi efficace, parce que le nombre N ne dépend que des divisions euclidiennes successives : on obtient, en plus, u et v vérifiant $au + bv = 1$.

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.

Exercice 10

1. $a = 4$ n'engendre pas Z_5^* (car $4^3 = 4 \mod 5$). En revanche, 2 engendre Z_5^* donc est primitif.
2. Bob envoie
$$k_B = a^B \mod p = 3$$
   Alice doit calculer $k = (k_B)^A \mod p = 4$ et doit envoyer à Bob ($k_A = a^A \mod p, kx$). Ainsi, Alice envoie le message

3. Bob décrypte : tout d'abord, il calcule lui-même k en utilisant $k_A = a^A \mod p$ envoyé par Alice et en calculant $k = k_A^B \mod p$:

$$k = 4^3 \mod 5 = 4$$

Il doit désormais calculer l'inverse de k modulo p, par l'algorithme d'Euclide étendue; il obtient comme inverse $k^{-1} = 4$. Il décrypte alors le message envoyer par Alice ($y = 2$) en calculant $k^{-1}y \mod p$, c'est-à-dire :

$$k^{-1}y = 4 \times 1 \mod 5 = 4$$

Ainsi, Bob a décrypté le message $x = 4$.

Exercice 11

1. (a) $19 = 16 + 2 + 1$, donc

$$a^{19} = a^{16}a^2a = a^{2^{2^{2^2}}} \times a^2 \times a$$

On effectue ainsi 7 multiplications, au lieu de 18.

(b) On aura alors

$$a^n = \prod_{j=0}^{k} a^{b_j 2^j} = \prod_{j=0}^{k} (a^{b_j})^{j^{j\cdots}}$$

2. (a) On utilise comme invariant de boucle, en notant $N_0 = N$ avant la boucle : $Res * x^N = x^{N_0}$. Alors, à la sortie de boucle, $N = 0$ et donc $Res = x^{N_0}$.

(b) Dans le pire cas, en base 2, N s'écrit $N = \sum_{k=0}^{p} 2^k$. Mais alors, dans ce cas, à chaque étape on effectue une étape $Res * x$, et une étape $x = x * x$. Soit 2 étapes pour chaque bit, et donc $2(p+1)$ étapes. Ainsi la complexité dans le pire des cas est $2(\log_2(n) + 1)$, au lieu de $n - 1$.

3. On obtient la même fonction, où Y = N.

Exercice 12

Rappelons qu'on effectue des calculs sur les polynômes, modulo $m(X) = X^8 + X^4 + X^3 + X + 1$.

On note $A(X) = X^7 + X^6 + X^3 + 1$, $B(X) = X^7 + X^3 + X^2 + 1$ et $C(X) = X^5 + X^4 + X^3 + X + 1$.

On calcule $A(X)B(X) + C(X)$, dans $Z_2[X]$ et on fait modulo $m(x)$ à la fin.

On a alors, dans $\mathbb{Z}_2[X]$:

$$\begin{aligned} A(X)B(X) + C(X) &= (X^7 + X^6 + X^3 + 1)(X^7 + X^3 + X^2 + 1) + C(X) \\ &= X^{14} + X^{10} + X^9 + X^7 + X^{13} + X^9 + X^8 + X^6 + X^{10} + X^6 + X^5 + X^3 + X^7 + X^3 + X^2 + 1 + C(X) \\ &= X^{14} + X^{13} + X^8 + X^5 + X^2 + 1 + X^5 + X^4 + X^3 + X + 1 \\ &= X^{14} + X^{13} + X^8 + X^4 + X^3 + X^2 + X + 1 \end{aligned}$$

On passe modulo $m(x)$, en effectuant la division euclidienne. On obtient alors :

$$A(X)B(X) + C(X) = m(X)(X^6 + X^5 + X^2) + (X^7 + X^6 + X^4 + X^1 + X^0)$$

Ainsi, le résultat obtenu est le reste précédent, soit 11010011.

Exercice 15

1. (a) On a, pour k grand :
$$\mathrm{N}(k) \approx \pi(2^k) - \pi(2^{k-1})$$
soit, en utilisant le théorème des nombres premiers démontrés par Hadamard et la Vallée Poussin :
$$\begin{aligned}\mathrm{N}(k) &\approx \frac{2^k}{\ln(2^k)} - \frac{2^{k-1}}{\ln(2^{k-1}} \\ &\approx \frac{2^k}{k\ln(2)} - \frac{2^{k-1}}{(k-1)\ln(2)} \\ &\approx 2^{k-1}\frac{2(k-1)-k}{k(k-1)\ln(2)} \\ &\approx 2^{k-1}\frac{k-2}{k(k-1)\ln(2)} \approx \frac{2^{k-1}}{k\ln(2)}\end{aligned}$$

   (b) On choisit aléatoirement un nombre impairs compris entre 2^{k-1} et $2^k - 1$ inclus. Il y a $\frac{2^k-2^{k-1}}{2}$ nombres impairs. On applique alors la probabilité qu'il soit premier est (pour k grand et en utilisant l'approximation vue précédemment) :
$$\begin{aligned}\mathrm{P} &= \frac{\mathrm{N}(k)}{\frac{2^k-2^{k-1}}{2}} \\ &\approx \frac{\frac{2^{k-1}}{k\ln(2)}}{2^{k-1}-2^{k-2}} \\ &\approx \frac{2}{k\ln(2)}\end{aligned}$$

2. (a) Cf cours.

   (b) On est sûr que le nombre est composé si l'algorithme renvoie faux. En revanche, s'il renvoie vrai, c'est soit que le nombre n est premier, soit qu'il ne l'est pas mais qu'on a tiré l'un des entiers a qui renvoie $f(a,b)$ vrai.

   (c) On suppose que n est composé. Puisqu'on choisit de manière uniforme l'entier a, l'algorithme renvoie vrai si on tombe sur l'un des entiers qui renvoie $f(n,a)$ vrai. Mais alors, par hypothèse de construction de f, on a :
$$\mathrm{P}_{n \text{ composé}}(f(a,n) \text{ renvoie vrai}) \leqslant \frac{\frac{n-1}{4}}{n} \leqslant \frac{1}{4}$$

   (d) On choisit aléatoirement l'entier a, et on effectue m fois la boucle. On a alors, en utilisant la question précédente,
$$\mathrm{P}_{n \text{ composé}}(\text{renvoie vrai}) = \prod_{i=1}^{m} \mathrm{P}_{n \text{ composé}}(f(a,n) \text{ renvoie vrai}) \leqslant \frac{1}{4^m}$$

3. On note C l'événement n est composé, et A l'événement "l'algorithme renvoie vrai". Alors on cherche :
$$\mathrm{P}_{\mathrm{A}}(\mathrm{C})$$
En utilisant les questions 1)a) et 2)d), on a alors :
$$\begin{aligned}\mathrm{P}_{\mathrm{A}}(\mathrm{C}) &= \frac{\mathrm{P}(\mathrm{A}\cap\mathrm{C})}{\mathrm{P}(\mathrm{A})} \\ &= \frac{\mathrm{P}(\mathrm{C})}{\mathrm{P}(\mathrm{A})}\mathrm{P}_{\mathrm{C}}(\mathrm{A}) \qquad \text{par la formule de Bayes} \\ &\leqslant \frac{k\ln(2)}{2\times 4^m}\end{aligned}$$

Par exemple, pour $k = 1024$ et $m = 50$, on obtient

$$\mathrm{P_A(C)} \leqslant 2,5 \times 10^{-28}$$