Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22
Travaux dirigés
Alain Kraus

Correction des exercices - Chapitre I

Cryptosystèmes à clés publiques

Exercice 1 (Cryptosystème RSA)

1) On a $n = 5 \times 53$ donc $\varphi(n) = 208$. Il s'agit de déterminer l'inverse de 139 modulo 208. En utilisant l'algorithme d'Euclide, on obtient le tableau suivant :

	1	2	69	
208	139	69	1	0
1	0	1	-2	
0	1	-1	3	

On en déduit l'égalité $3 \times 139 - 2 \times 208 = 1$, donc 3 est l'inverse de 139 modulo 208. Par suite, la clé secrète est $(3, 208)$.

Supposons $n = 3599$. On a les égalités

$$n = 3600 - 1 = 60^2 - 1 = 59 \times 61,$$

d'où $\varphi(n) = 3480$. En utilisant l'algorithme d'Euclide, on obtient l'égalité

$$4 \times 3480 - 449 \times 31 = 1,$$

donc l'inverse de 31 modulo 3480 est 3031. La clé secrète est ainsi $(3031, 3480)$.

2) On a $n = 11 \times 17$, $\varphi(n) = 160$. L'inverse de 107 modulo 160 est 3 (algorithme d'Euclide). Par suite, le message m que Bob souhaite transmettre à Alice est

$$m = 9^3 \text{ mod. } 187 = 168 \text{ mod. } 187.$$

3) Soit (e, n) la clé publique d'Alice. On a $n = pq$ et $p < q$ premiers. On a les relations

$$\varphi(n) = (p-1)(q-1) = 88 \quad \text{et} \quad 3e \equiv 1 \text{ mod. } 88.$$

L'égalité $87 = 3 \times 29$ implique $e \equiv -29 \equiv 59 \text{ mod. } 88$, d'où $e = 59$. Déterminons n. En considérant les factorisations de 88 comme produit de deux entiers, on en déduit que

le couple (p, q) appartient à l'ensemble $\{(2, 89), (5, 23)\}$, ce qui correspond à $n = 178$ ou $n = 115$. Par ailleurs, d'après les hypothèses faites, on a la congruence

$$7^3 \equiv 113 \text{ mod. } n.$$

(Avec les notations du cours, on a $d = 3$ et dans $\mathbb{Z}/n\mathbb{Z}$ on a les égalités $x_0 = 113$, $7 = x_0^e$ puis $7^3 = 113$.) Ainsi n divise l'entier

$$7^3 - 113 = 343 - 113 = 230 = 2 \times 115,$$

d'où $n = 115$, puis $(e, n) = (59, 115)$.

Exercice 2 (Racines carrées dans $\mathbb{F}_p$)

1) D'après le critère d'Euler[(1)], on a dans $\mathbb{F}_p^*$ l'égalité $a^{\frac{p-1}{2}} = 1$. Il en résulte que l'on a

$$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} a = a,$$

d'où l'assertion.

2) Parce que $\mathbb{F}_p$ est un corps, l'égalité $a^{\frac{p-1}{2}} = 1$ entraîne $a^{\frac{p-1}{4}} = \pm 1$ (p est congru à 1 modulo 4).
Si l'on a $a^{\frac{p-1}{4}} = 1$, en posant $x = \pm a^{\frac{p+3}{8}}$, on obtient $x^2 = a^{\frac{p+3}{4}} = a$.
Supposons $a^{\frac{p-1}{4}} = -1$. D'après la congruence $p \equiv 5$ mod. 8, on a l'égalité[(2)] $\left(\frac{2}{p}\right) = -1$, autrement dit, on a dans $\mathbb{F}_p$ l'égalité

$$2^{\frac{p-1}{2}} = -1.$$

Posons $x = \pm 2a.(4a)^{\frac{p-5}{8}}$. On vérifie alors que l'on a

$$x^2 = 4a^2.(4a)^{\frac{p-5}{4}} = a^{\frac{p+3}{4}} 2^{\frac{p-1}{2}} = -a^{\frac{p+3}{4}} = -a^{\frac{p-1}{4}} a = a.$$

---

(1) Ce critère est le suivant. Soit $p \geq 3$ un nombre premier. Pour tout entier n, on a

$$n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \text{ mod. } p,$$

où $\left(\frac{n}{p}\right)$ est le symbole de Legendre. Si p ne divise pas n, on a $\left(\frac{n}{p}\right) = 1$ si n est un carré modulo p. On a $\left(\frac{n}{p}\right) = -1$ si n n'est pas un carré modulo p. On a $\left(\frac{n}{p}\right) = 0$ si p divise n. Le critère d'Euler est une conséquence du fait que $\mathbb{F}_p^*$ est un groupe cyclique, dont le sous-groupe des carrés est d'ordre $(p-1)/2$.

(2) Rappelons que l'on a $\left(\frac{2}{p}\right) = 1$ si et seulement si $p \equiv \pm 1$ mod. 8. On a aussi $\left(\frac{-1}{p}\right) = 1$ si et seulement si $p \equiv 1$ mod. 4 (si $p \neq 2$).

3) Parce que $\mathbb{F}_p^*$ est cyclique, G est l'unique sous-groupe de $\mathbb{F}_p^*$ d'ordre 2^e et il est formé des éléments $x \in \mathbb{F}_p^*$ tels que $x^{2^e} = 1$. On a

$$a^{p-1} = \big(a^q\big)^{2^e} = 1,$$

donc a^q est dans G. Notons G^2 l'ensemble des carrés de G. C'est l'unique sous-groupe de G d'ordre 2^{e-1} (considérer le morphisme $G \to G$ qui à x associe x^2, dont le noyau est d'ordre 2). Ainsi, pour tout $x \in G$, x est dans G^2 si et seulement si $x^{2^{e-1}} = 1$. L'élément a étant un carré dans $\mathbb{F}_p$, on a

$$a^{\frac{p-1}{2}} = \big(a^q\big)^{2^{e-1}} = 1,$$

donc a^q appartient à G^2.

4) D'après la question précédente, il existe un entier pair u tel que l'on ait $a^q = z^u$ avec $0 \leq u < 2^e$, ce qui entraîne l'assertion (si $u = 0$ on prend $k = 0$, sinon on prend $k = 2^e - u$). On obtient ainsi les égalités $x^2 = a^{q+1}z^k = a(a^q z^k) = a$.

5.1) Considérons les polynômes f_t de $\mathbb{F}_p[X]$ de la forme $X^2 - tX + a$ où $t \in \mathbb{F}_p$, dont le discriminant est $t^2 - 4a$. Déterminons le nombre de polynômes f_t qui sont réductibles dans $\mathbb{F}_p[X]$. Il y a deux éléments $t \in \mathbb{F}_p$ tels que f_t possède une racine double, à savoir $t = \pm 2w$ où $w^2 = a$ et $w \in \mathbb{F}_p$, auquel cas on a $f_t = (X - w)^2$ ou $f_t = (X + w)^2$.
Par ailleurs, le polynôme f_t a deux racines distinctes dans $\mathbb{F}_p$ si et seulement si il existe $u \in \mathbb{F}_p$ non nul et distinct de $\pm w$, tel que l'on ait

$$f_t = (X - u)\Big(X - \frac{a}{u}\Big).$$

Il y a $(p-3)/2$ polynômes de cette forme. Il y en a donc $(p+1)/2$ qui sont réductibles sur $\mathbb{F}_p$. Parce qu'il y a p polynômes f_t, on en déduit qu'il y en a $(p-1)/2$ qui sont irréductibles sur $\mathbb{F}_p$, i.e. dont le discriminant n'est pas un carré dans $\mathbb{F}_p$, d'où le résultat.

5.2) L'anneau quotient considéré est un corps de cardinal p^2, car $X^2 - tX + a$ est un polynôme irréductible dans $\mathbb{F}_p[X]$. Ses deux racines sont α et α^p, d'où $\alpha^{p+1} = a$. On en déduit que l'on a

$$\big(\alpha^{\frac{p+1}{2}}\big)^2 = a.$$

Parce que a est un carré dans $\mathbb{F}_p$, $\alpha^{\frac{p+1}{2}}$ est donc aussi dans $\mathbb{F}_p$, car le polynôme $X^2 - a \in \mathbb{F}_p[X]$ a au plus deux racines dans $\mathbb{F}_{p^2}$.

6) D'après la loi de réciprocité quadratique[(3)], on a les égalités des symboles de Legendre

---

[(3)] Rappelons son énoncé. Soient p et q des nombres premiers impairs distincts. On a

$$\Big(\frac{p}{q}\Big) = (-1)^{\frac{(p-1)(q-1)}{4}}\Big(\frac{q}{p}\Big).$$

Ainsi, on a $\big(\frac{p}{q}\big) = \big(\frac{q}{p}\big)$ si p ou q est congru à 1 modulo 4, sinon on a $\big(\frac{p}{q}\big) = -\big(\frac{q}{p}\big)$.

$$\left(\frac{5}{29}\right) = \left(\frac{29}{5}\right) = \left(\frac{4}{5}\right) = 1,$$

donc 5 est un carré dans $\mathbb{F}_{29}$.

Utilisons alors la première méthode. Le groupe $\mathbb{F}_{29}^*$ est d'ordre $28 = 2^2.7$. En reprenant les notations précédentes, on a $e = 2$ et $q = 7$, et G est cyclique d'ordre 4. Puisque l'on a $12^2 \equiv -1$ mod. 29, on peut prendre $z = 12$. Il existe donc un entier pair k tel que l'on ait $0 \leq k < 4$ et $5^7.12^k \equiv 1$ mod. 29, et l'on vérifie que $k = 2$. Il en résulte que

$$x = 5^4.12 = 18 \text{ mod. } 29$$

est une racine carrée de 5 dans $\mathbb{F}_{29}$, l'autre racine carrée étant la classe de $11 \in \mathbb{F}_{29}$.

Utilisons l'algorithme de Cipolla. On peut prendre $t = 1$. En effet, $t^2 - 20 = -19$ qui n'est pas un carré dans $\mathbb{F}_{29}$. Soit α une racine dans $\mathbb{F}_{29^2}$ du polynôme $X^2 - X + 5$. En utilisant l'égalité $\alpha^2 - \alpha + 5 = 0$, on vérifie que l'on a $\alpha^{15} = 11$, d'où le fait que 11 et 18 soient les deux racines carrées de 5 dans $\mathbb{F}_{29}$.

Exercice 3

1.1) Soit a un élément de B. Pour tout $i = 1, \cdots, r$, on a $a^2 \equiv 1$ mod. $p_i^{n_i}$, ce qui entraîne $a^2 \equiv 1$ mod. n i.e. a est dans A. Inversement, soit a un élément de A. Le pgcd des entiers $a - 1$ et $a + 1$ est 1 ou 2. Puisque n est impair, pour tout $i = 1, \cdots, r$, l'entier $p_i^{n_i}$ divise donc $a - 1$ ou $a + 1$. Par suite, a est dans B. (On peu aussi utiliser le fait que $(\mathbb{Z}/p_i^{n_i}\mathbb{Z})^*$ est cyclique car $p_i \neq 2$; si $a \in A$, on a $a^2 \equiv 1$ mod. $p_i^{n_i}$, d'où $a_i \equiv \pm 1$ mod. $p_i^{n_i}$ et a est dans B.) On a donc $A = B$.

1.2) D'après le théorème chinois, pour tout système de signes $(\varepsilon_1, \cdots, \varepsilon_r)$, il existe $a \in \mathbb{Z}$, unique modulo $n\mathbb{Z}$, vérifiant les congruences

$$a \equiv \varepsilon_i \text{ mod. } p_i^{n_i} \quad \text{pour} \quad i = 1, \cdots, r.$$

Il y a 2^r tels systèmes de signes. L'ensemble des classes modulo $n\mathbb{Z}$ des éléments de B est donc de cardinal 2^r. Puisque l'on a $A = B$, on obtient $|S| = 2^r$.

2.1) Si $n = 2$, on a $S = \{\overline{1}\}$ et si $n = 4$, on a $S = \{\overline{1}, \overline{3}\}$.

2.2) Considérons un entier a tel que $a^2 \equiv 1$ mod. 2^t. Le pgcd de $a - 1$ et $a + 1$ est 2. Il en résulte que $a + 1$ ou bien $a - 1$ est divisible par 2^{t-1}. Autrement dit, on a $a \equiv \pm 1$ mod. 2^{t-1}. Supposons $a \not\equiv \pm 1$ mod. 2^t. Dans ce cas, il existe $u \in \mathbb{Z}$ impair tel que $a = \pm 1 + u2^{t-1}$, ce qui conduit à la congruence $a \equiv \pm 1 + 2^{t-1}$ mod. 2^t, d'où le résultat annoncé.

3) Posons $n = 2^t d$, où d est impair. D'après le théorème chinois les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/2^t\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ sont isomorphes. Le cardinal de S est donc le nombre de couples de

l'anneau produit $\mathbb{Z}/2^t\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ dont le carré vaut 1. Compte tenu de ce qui précède, si r est le nombre de facteurs premiers de d, on a donc

$$|S| = \begin{cases} 2^r & \text{si } t = 0 \text{ ou } t = 1 \\ 2^{r+1} & \text{si } t = 2 \\ 2^{r+2} & \text{si } t \geq 3. \end{cases}$$

4) Supposons $n = 128 = 2^7$. D'après la deuxième question, on a

$$S = \left\{\overline{1}, \overline{63}, \overline{65}, \overline{127}\right\}.$$

Supposons $n = 735 = 3 \times 5 \times 7^2$. L'équation $x^2 = 1$ possède huit solutions dans l'anneau $\mathbb{Z}/735\mathbb{Z}$. Pour les trouver, il faut résoudre les huit systèmes de trois congruences (question 1)

$$x \equiv \pm 1 \text{ mod. } 3, \quad x \equiv \pm 1 \text{ mod. } 5, \quad x \equiv \pm 1 \text{ mod. } 49.$$

En réalité, il suffit d'en résoudre quatre par un choix convenable de systèmes de signes, les autres solutions étant les opposées des précédentes. Il suffit donc d'examiner les triplets de signes $(1,1,1)$, $(1,-1,-1)$, $(1,1,-1)$ et $(1,-1,1)$. Indiquons dans ce qui suit des solutions particulières de ces systèmes, obtenues en utilisant l'algorithme d'Euclide.
Pour le triplet $(1,1,1)$, on a directement $x = 1$.
Pour le triplet $(1,-1,-1)$, on résoud le système

$$x \equiv 1 \text{ mod. } 3 \quad \text{et} \quad x \equiv -1 \text{ mod. } 245.$$

On a la relation de Bézout $82 \times 3 - 245 = 1$, d'où (cf. la démonstration du théorème chinois)

$$x = -82 \times 3 - 245 = -491 \equiv 244 \text{ mod. } 735$$

est une solution particulière de ce système.
Pour le triplet $(1,1,-1)$, on résoud le système

$$x \equiv 1 \text{ mod. } 15 \quad \text{et} \quad x \equiv -1 \text{ mod. } 49.$$

On a $-13 \times 15 + 4 \times 49 = 1$, d'où $x = 13 \times 15 + 4 \times 49 = 391$.
Pour le triplet $(1,-1,1)$, on résoud le système

$$x \equiv 1 \text{ mod. } 147 \quad \text{et} \quad x \equiv -1 \text{ mod. } 5.$$

On a $-2 \times 147 + 59 \times 5 = 1$, d'où $x = 59 \times 5 + 2 \times 147 = 589$.
Il en résulte que l'on a

$$S = \left\{\overline{1}, \overline{146}, \overline{244}, \overline{344}, \overline{391}, \overline{491}, \overline{589}, \overline{734}\right\}.$$

Exercice 4 (Cryptosystème de Massey-Omura)

1) On a les égalités

$$c^{y_B} = \left(b^{y_A}\right)^{y_B} = \left(a^{x_B y_A}\right)^{y_B} = \left(m^{x_A y_A}\right)^{x_B y_B}.$$

Il existe deux entiers naturels u et v tels que l'on ait $x_A y_A = 1 + un$ et $x_B y_B = 1 + vn$. Soit e l'élément neutre de G. Puisque G est d'ordre n, on a $m^{un} = m^{vn} = e$. Par suite, on obtient

$$c^{y_B} = \left(m^{1+un}\right)^{1+vn} = m.$$

2) On a dans cet exemple $n = 18$. Supposons que Bob choisisse l'élément $x_B = 7$. Dans ce cas, il renvoie à Alice l'élément $b = \overline{2}^7 = 14$ mod. 19. On vérifie que l'on a $y_A = 11$ car on a $5 \times (-7) + 18 \times 2 = 1$. Alice renvoie ainsi à Bob l'élément $c = \overline{14}^{11}$. Par ailleurs, vu l'égalité $7 \times 13 - 5 \times 18 = 1$, on a $y_B = 13$. Ainsi Bob effectue l'opération $(14^{11})^{13}$ modulo 19. On a $11 \times 13 \equiv 17$ mod. 18. D'après le petit théorème de Fermat, on a donc

$$(14^{11})^{13} \equiv 14^{17} \text{ mod. } 19.$$

On en déduit que l'on a $m = 14^{-1}$ mod. $19 = 15$ mod. 19 (on a $-4 \times 14 + 3 \times 19 = 1$) i.e. $m = 15 \in \mathbb{F}_{19}^*$.

Exercice 5 (Algorithme de El Gamal)

1) Le polynôme $X^4 + X + 1 \in \mathbb{F}_2[X]$ n'a pas de racines dans $\mathbb{F}_2$ et n'est pas divisible par $X^2 + X + 1$ qui est le seul polynôme irréductible de degré 2 de $\mathbb{F}_2[X]$, donc $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$ et K est un corps. Le groupe K^* est d'ordre 15. On a $\alpha^4 = \alpha + 1$, d'où l'on déduit que α^3 et α^5 sont distincts de 1, ce qui entraîne que l'ordre de α dans K^* est 15.
2) Il transmet le couple $\left(\alpha^3, (1+\alpha)(1+\alpha^2)^3\right)$ i.e. $\left(\alpha^3, \alpha^3 + \alpha^2 + 1\right)$.
3) On cherche l'entier a tel que $1 \leq a \leq 14$ et que $1 + \alpha^2 = \alpha^a$. On remarque pour cela que l'on a $(1+\alpha^2)^2 = 1 + \alpha^4 = \alpha$. De l'égalité $(1+\alpha^2)^{16} = 1 + \alpha^2$ (on a $x^{16} = x$ pour tout $x \in K$), on déduit que l'on a $1 + \alpha^2 = \alpha^8$ i.e. on a $a = 8$. On a $\alpha^{15} = 1$, d'où

$$\alpha^{ax} = \alpha^{24} = \alpha^9.$$

Par définition, si m est le message envoyé par Bob, on a

$$m\alpha^{ax} = \alpha^3 + \alpha^2 + \alpha.$$

On a $\alpha^{15} = 1$, donc l'inverse de α^{ax} est α^6, autrement dit, on a

$$\left(\alpha^9\right)^{-1} = \alpha^2 + \alpha^3.$$

On a donc $m = (\alpha + \alpha^2 + \alpha^3)(\alpha^2 + \alpha^3)$, d'où $m = \alpha^2$.

Exercice 6 (Protocole de Diffie-Hellman)

1) Le polynôme $X^3 + 2X + 1 \in \mathbb{F}_3[X]$ est irréductible sur $\mathbb{F}_3$ car il n'a pas de racines dans $\mathbb{F}_3$ et son degré est 3, donc K est un corps de cardinal 27.
Le groupe K^* est d'ordre 26. Les ordres de ses éléments autres que l'élément neutre, sont donc 2, 13 ou 26. En fait, -1 est le seul élément d'ordre 2 de K^*, car par exemple ± 1 sont les seules racines du polynôme $X^2 - 1 \in K[X]$. On a $\alpha^3 = \alpha - 1$, d'où $\alpha^9 = \alpha^3 - 1$ (car K est de caractéristique 3) i.e. $\alpha^9 = \alpha + 1$, d'où $\alpha^{12} = \alpha^2 - 1$ puis $\alpha^{13} = -1$ et notre assertion.
2) On a $\alpha^4 = \alpha^2 - \alpha$ et $\alpha^5 = 2\alpha^2 + \alpha + 2$, d'où $b = 5$.
3) La clé secrète d'Alice et Bob est donc $\left(\alpha^9\right)^5 = \alpha^{45}$. Déterminons ses coordonnées dans la base $(1, \alpha, \alpha^2)$ de K sur $\mathbb{F}_3$. En utilisant l'égalité $\alpha^{13} = -1$, on obtient

$$\alpha^{45} = \alpha^{39}\alpha^6 = -\alpha^6.$$

Par suite, on a

$$\alpha^{45} = -(\alpha^2 + \alpha + 1).$$

Notons que la clé secrète d'Alice et Bob est aussi $(\alpha^b)^9 = (2 + \alpha + 2\alpha^2)^9$. On retrouve le résultat précédent en remarquant que l'on a

$$(2 + \alpha + 2\alpha^2)^9 = 2^9 + \alpha^9 + (2\alpha^2)^9 = 2 + \alpha^9 + 2\alpha^{18}.$$

On a $\alpha^9 = 1 + \alpha$ et $\alpha^{18} = 1 + 2\alpha + \alpha^2$, d'où $(\alpha^b)^9 = -(\alpha^2 + \alpha + 1)$.

Exercice 7 (Protocole de Diffie-Hellman dans un corps de cardinal p^2)

1) On a $p \equiv 3$ mod. 4, donc -1 n'est pas un carré dans $\mathbb{F}_p$ i.e. $X^2 + 1$ est irréductible dans $\mathbb{F}_p[X]$. Il en résulte que K est un corps à p^2 éléments.

2.1) Il s'agit de démontrer que l'on a l'implication

$$(a + ib)^m \in \mathbb{F}_p \Longrightarrow p + 1 \text{ divise } m. \tag{1}$$

Soit d le pgcd de m et $p + 1$. Il existe u et $v \in \mathbb{Z}$ tels que $d = um + v(p + 1)$. Puisque K^* est d'ordre $p^2 - 1$, on a $\left((a + ib)^{p+1}\right)^{p-1} = 1$, donc $(a + ib)^{p+1}$ appartient $\mathbb{F}_p$. Il en résulte que l'on a

$$\left((a + ib)^m\right)^u \left((a + ib)^{p+1}\right)^v = (a + ib)^d \in \mathbb{F}_p. \tag{2}$$

Vérifions alors que l'on a $d = p + 1$. Supposons le contraire. L'entier d divise $p + 1$ qui est une puissance de 2, donc d divise $\frac{p+1}{2}$. D'après (2), on en déduit que

$$(a + ib)^{\frac{p+1}{2}} \in \mathbb{F}_p.$$

Par ailleurs, le carré de cet élément est a^2+b^2. En effet, p étant congru à 3 modulo 4, on a $i^p=-i$, et vu que l'on a $a^p=a$ et $b^p=b$, on obtient

$$(a+ib)^{p+1}=(a+ib)^p(a+ib)=(a^p+b^pi^p)(a+ib)=(a-ib)(a+ib)=a^2+b^2.$$

Cela conduit à une contradiction, car par hypothèse a^2+b^2 étant un générateur de $\mathbb{F}_p^*$, ce n'est pas un carré dans $\mathbb{F}_p$ (un carré est d'ordre divisant $\frac{p-1}{2}$). On a donc $d=p+1$, par suite $p+1$ divise m. Cela prouve l'implication (1).

2.2) Considérons alors un entier $n\geq 1$ tel que

$$(a+ib)^n=1.$$

D'après (1), $p+1$ divise n. Soit $r\in\mathbb{Z}$ tel que $n=(p+1)r$. L'égalité $(a+ib)^{p+1}=a^2+b^2$ entraîne alors

$$(a^2+b^2)^r=1.$$

Parce que a^2+b^2 est un générateur de $\mathbb{F}_p^*$, $p-1$ divise r, donc p^2-1 divise n. Ainsi $a+ib$ est d'ordre p^2-1, d'où l'assertion.

3) Soit L un corps fini de cardinal q. Si q est une puissance de 2, tout élément de L est un carré. Supposons q impair. Considérons un élément $a\in L$. L'ensemble L^2 des carrés dans L est de cardinal $\frac{q+1}{2}$. Par ailleurs, $S=\{a-x^2\mid x\in L\}$ est aussi de cardinal $\frac{q+1}{2}$. On en déduit que $S\cap L^2$ n'est pas vide. Il existe donc x et y de L tels que l'on ait $a-x^2=y^2$, d'où le résultat.

4) Montrons que 13 est un générateur de $\mathbb{F}_{31}^*$. Pour cela, on vérifie que l'on a

$$13^2\equiv 14 \text{ mod. } 31,\quad 13^3\equiv -4 \text{ mod. } 31,\quad 13^5\equiv 6 \text{ mod. } 31,$$

$$13^6\equiv 16 \text{ mod. } 31,\quad 13^{10}\equiv 5 \text{ mod. } 31,\quad 13^{15}\equiv -1 \text{ mod. } 31,$$

ce qui entraîne l'assertion. Par ailleurs, on a $17\equiv -14\equiv -13^2$ mod. 31. Parce que 13 est un générateur de $\mathbb{F}_{31}^*$, l'ordre de $13^2\in\mathbb{F}_{31}^*$ est 15 et donc l'ordre de -13^2 vaut 30. Par suite, 17 est un générateur de $\mathbb{F}_{31}^*$.

5.1) Conformément au protocole de Diffie-Hellman, la clé commune de chiffrement est

$$\alpha=(1+19i)^{193}.$$

On a $193=6\times 31+7$ et $i^{31}=-i$, d'où $(1+19i)^{31}=1-19i$. On obtient

$$\alpha=(1-19i)^6(1+19i)^7=(1+19^2)^6(1+19i).$$

On a $1+19^2=362\equiv 21$ mod. 31, d'où

$$(1+19^2)^6\equiv 21^6\equiv 2 \text{ mod. } 31.$$

On en déduit que l'on a

$$\alpha = 2(1 + 19i) = 2 + 7i.$$

5.2) Alice doit envoyer à Bob l'élément $\beta = (4+i)^{193}$. On a $(4+i)^{31} = 4 - i$ et $17^6 = 8$. On obtient

$$\beta = (4-i)^6(4+i)^7 = 17^6(4+i) = 8(4+i) = 1 + 8i.$$

Exercice 8 (Cryptosystème de Rabin)

1) D'après l'hypothèse faite, on a $22^2 \equiv 1$ mod. n. Ainsi, n divise $22^2 - 1 = 3.7.23$. Par ailleurs, Alice recevant le cryptogramme 2, il en résulte que 2 est un carré modulo n. En particulier, 2 est un carré modulo p et q, donc p et q sont distincts de 3. On obtient $n = 7.23 = 161$.

2) Il s'agit de résoudre l'équation $x^2 = 2$ dans l'anneau $\mathbb{Z}/161\mathbb{Z}$. On détermine pour cela les racines carrées de 2 modulo 7 et de 2 modulo 23. Les deux racines carrées de 2 dans $\mathbb{F}_7^*$ sont ± 3. Parce que 23 est congru à 3 modulo 4, on en déduit directement que $\pm 2^6$ sont les deux racines carrées de 2 dans $\mathbb{F}_{23}^*$ (voir par exemple l'exercice 2). On a $64 \equiv 18$ mod. 23. On est donc amené à résoudre les deux systèmes de congruences (cf. l'exemple 1.3 du cours)

$$\begin{cases} x \equiv 3 \text{ mod. } 7 \\ x \equiv 18 \text{ mod. } 23 \end{cases} \quad \text{et} \quad \begin{cases} x \equiv 3 \text{ mod. } 7 \\ x \equiv -18 \text{ mod. } 23. \end{cases}$$

En utilisant l'égalité $10 \times 7 - 3 \times 23 = 1$, on obtient comme solutions particulières respectivement $x = 87$ et $x = 143$. Il en résulte que les quatre messages décryptés possibles dans $\mathbb{Z}/161\mathbb{Z}$ sont 18, 74, 87 et 143.

Exercice 9 (Sac à dos)

Soit $(v_i)_{0 \leq i \leq k}$ suite finie d'entiers super croissante. Par définition, cela signifie que l'on a

$$0 < v_0 < v_1 < \cdots < v_k \quad \text{et} \quad v_i > \sum_{j=0}^{i-1} v_j \quad \text{pour tout } i \text{ tel que } 1 \leq i \leq k.$$

Pour tout entier V (le volume), le problème du sac à dos relatif à la suite $(v_i)_{0 \leq i \leq k}$ et à V est facile à résoudre. Il s'agit de déterminer s'il existe des entiers a_i égaux à 0 ou 1 tels que l'on ait

$$V = \sum_{i=0}^{k} a_i v_i. \tag{1}$$

Autrement dit, on cherche s'il existe ou non un sous-ensemble I de $\{0, \cdots, k\}$ tel que l'on ait l'égalité

$$V = \sum_{i \in I} v_i.$$

Ce problème possède au plus une solution (car la suite est supposée super croissante). Rappelons comment l'on procède. Parmi les entiers v_i on détermine le plus grand inférieur ou égal à V. Si v_{i_0} est cet entier, alors si le problème a une solution, nécessairement i_0 est dans I. On recommence de même avec l'entier $V - v_{i_0}$. On continu ainsi jusqu'à obtenir un entier v_{i_j} plus petit ou égal à la différence obtenue. S'il y a égalité, on a déterminé l'unique solution du problème. S'il n'y a pas égalité, le problème n'a pas de solutions. Si l'on trouve une suite (a_i) réalisant la condition (1), on dit parfois que l'entier binaire $n = (a_k a_{k-1} \cdots a_1 a_0)_2$ est solution du problème.

1) La suite $(2, 3, 7, 20, 35, 69)$ est super croissante et $n = (010110)_2$ est la solution, qui correspond à l'égalité $45 = 35 + 7 + 3$.
Il en est de même de la suite $(1, 2, 5, 9, 20, 49)$. On constate qu'avec l'entier $V = 73$ le problème n'a pas de solution.
La suite $(1, 3, 7, 12, 22, 45)$ ne l'est pas. Dans ce cas, il y a exactement deux solutions $(110000)_2$ et $(101110)_2$.
La suite $(4, 5, 10, 30, 50, 101)$ est super croissante et l'on trouve la solution $(111010)_2$.

2) On a $v_1 > v_0$. Si pour $i \geq 1$, v_i est plus grand que la somme des i premiers termes, on a les inégalités

$$v_{i+1} > 2v_i > \sum_{j=0}^{i} v_j,$$

d'où le résultat par récurrence.

3) On vérifie d'abord que la suite $(2^i)_{i \geq 0}$ est super croissante. Par ailleurs, soit $(a_i)_{i \geq 0}$ la suite super croissante telle que pour tout i le terme a_i soit le plus petit possible. Remarquons que cette suite existe. En effet, on prend $a_0 = 1$ et pour tout $i \geq 1$, a_i est le plus petit entier naturel vérifiant la condition

$$0 < a_0 < \cdots < a_{i-1} < a_i \quad \text{et} \quad a_i > \sum_{j=0}^{i-1} a_j.$$

Vérifions que l'on a $a_i = 2^i$. C'est vrai si $i = 0$. Soit i un entier ≥ 0. Supposons que l'on ait $a_j = 2^j$ pour tout j tel que $0 \leq j \leq i$. On a alors

$$a_{i+1} > \sum_{j=0}^{i} 2^j = 2^{i+1} - 1.$$

Par suite, le plus petit entier a_{i+1} possible est 2^{i+1}, d'où l'assertion.

Exercice 10 (Cryptosystème de Merkle-Hellman)

Rappelons d'abord le principe de ce cryptosystème. Les unités de message à transmettre sont des entiers binaires ayant disons k composantes. Chaque utilisateur choisit une suite d'entiers super croissante $(v_0, v_1, \cdots, v_{k-1})$, un entier m tel que

$$m > \sum_{i=0}^{k-1} v_i, \tag{1}$$

et un entier a tel que $1 \leq a < m$ et $\text{pgcd}(a, m) = 1$. Il détermine ensuite l'entier b tel que

$$1 \leq b < m \quad \text{et} \quad ab \equiv 1 \text{ mod. } m,$$

et pour tout $i = 0, \cdots, k-1$, l'entier w_i tel que

$$1 \leq w_i < m \quad \text{et} \quad w_i \equiv av_i \text{ mod. } m. \tag{2}$$

L'utilisateur garde secret les entiers v_i, m, a et b. La suite $(w_0, \cdots, w_{k-1})$ est sa clé publique.
Une personne souhaitant envoyer un message binaire $P = (\varepsilon_{k-1} \cdots \varepsilon_0)_2$ transmet à l'utilisateur l'entier

$$C = \sum_{i=0}^{k-1} \varepsilon_i w_i.$$

Afin de décrypter ce message l'utilisateur procède comme suit. Il calcule l'entier V tel que

$$0 \leq V < m \quad \text{et} \quad V \equiv bC \text{ mod. } m.$$

On a l'égalité

$$V = \sum_{i=0}^{k-1} \varepsilon_i v_i. \tag{3}$$

En effet, d'après (2), on a

$$bC = \sum_{i=0}^{k-1} \varepsilon_i b w_i \equiv \sum_{i=0}^{k-1} \varepsilon_i v_i \text{ mod. } m.$$

Par ailleurs, on a $0 \leq V < m$, et d'après l'inégalité (1), on a

$$0 \leq \sum_{i=0}^{k-1} \varepsilon_i v_i \leq \sum_{i=0}^{k-1} v_i < m,$$

d'où l'égalité (3). À l'aide de l'algorithme du sac à dos super croissant, appliqué avec la suite $(v_0, v_1, \cdots, v_{k-1})$, l'utilisateur peut alors retrouver le message P.

1) On vérifie que la suite $(v_0, \cdots, v_7) = (4, 5, 12, 23, 45)$ est super croissante, que l'on a $a = 381 = 3 \times 127$, puis

$$m = 400 > \sum_{i=0}^{4} v_i = 89 \quad \text{et} \quad \text{pgcd}(381, 400) = 1,$$

de sorte que les données proposées sont conformes au principe d'utilisation du cryptosystème.

2) On détermine l'entier b tel que $1 \leq b < 400$ et $381b \equiv 1 \text{ mod. } 400$. À l'aide de l'algorithme d'Euclide, on trouve que l'on a $b = 21$. Il s'agit ensuite de déterminer les entiers w_i définis par l'égalité (2) ci-dessus. On vérifie alors que la clé publique d'Alice est

$$(w_0, w_1, w_2, w_3, w_4) = (324, 305, 172, 363, 345).$$

3) On vérifie que l'on a

$$O = (01110)_2, \quad U = (10100)_2, \quad I = (01000)_2.$$

Pour chacun des trois messages $(\varepsilon_4\varepsilon_3\varepsilon_2\varepsilon_1\varepsilon_0)_2$ ci-dessus à envoyer, Bob transmet donc à Alice successivement le message

$$\sum_{i=0}^{4} \varepsilon_i w_i.$$

Il transmet ainsi les messages cryptés

$$C_1 = 363 + 172 + 305 = 840, \quad C_2 = 345 + 172 = 517, \quad C_3 = 363.$$

Afin de retrouver le mot OUI, Alice calcule les trois entiers V_i tels que

$$0 \leq V_i < 400 \quad \text{et} \quad V_i \equiv 21C_i \text{ mod. } 400.$$

On trouve

$$V_1 = 40, \quad V_2 = 57, \quad V_3 = 23.$$

Les égalités (3) qui correspondent à chacun des V_i sont respectivement

$$40 = 23 + 12 + 5, \quad 57 = 45 + 12, \quad 23 = 23,$$

et Alice peut alors retrouver le mot OUI.