Feuille d'exercices 8

Avertissement : tous les exercices ne seront pas traités durant les séances ; pour en suivre l'avancement veuillez consulter mon site personnel dans la rubrique *Forum*.

Cryptosystèmes

Exercice 1. — *Soit E la cubique définie sur $\mathbb{F}_{11}$ d'équation*

$$y^2 = x^3 + x + 6.$$

1. *Montrer que E est une courbe elliptique sur $\mathbb{F}_{11}$.*
2. *Déterminer l'ordre du groupe $E(\mathbb{F}_{11})$.*

   On constate que le point $P = (2, 7)$ appartient à $E(\mathbb{F}_{11})$. Bob souhaite envoyer le message $M = (9, 1) \in \mathbb{F}_{11} \times \mathbb{F}_{11}$ à Alice (M n'est pas un point de E) en utilisant le cryptosystème de Menezes-Vanstone associé au couple public (E, P). La clé secrète d'Alice est l'entier $s = 7$.
3. *Calculer la clé publique d'Alice.*
4. *Bob choisit aléatoirement l'entier $k = 6$. Quel est le message chiffré envoyé par Bob à Alice et comment Alice retrouve-t-elle le message M ?*

Exercice 2. — *Soit $G = E(\mathbb{F}_{41})$ où E est donné par $y^2 = x^3 + 2x + 1$. Soient $P = (0, 1)$ et $Q = (30, 40)$; en utilisant l'algorithme Baby step Giant step, trouver k tel que $Q = kP$.*

Exercice 3. — *Soit E une courbe elliptique sur $\mathbb{F}_q$ et soient $P, Q \in E(\mathbb{F}_q)$. On suppose que l'ordre N de P est premier avec q.*

1. *Montrer qu'il existe k tel que $Q = kP$ si et seulement si $NQ = O$ et l'accouplement de Weil vérifie $e_N(P, Q) = 1$.*
2. *Soit m tel que $E[N] \subset E(\mathbb{F}_{q^m})$ et on considère l'algorithme suivant :*
   (a) *on choisit aléatoirement un point $T \in E(\mathbb{F}_{q^m})$;*
   (b) *on calcule l'ordre M de T ;*
   (c) *soit $d = M \wedge N$ et $T_1 = \frac{M}{d}T$ de sorte que T_1 est d'ordre d qui divise N ;*
   (d) *on calcule $\zeta_1 = e_N(P, T_1)$ et $\zeta_2 = e_N(Q, T_1)$ qui appartiennent donc à $\mu_d \subset \mathbb{F}_{q^m}^\times$;*
   (e) *on résoud le logarithme discret $\zeta_2 = \zeta_1^k$ dans $\mathbb{F}_{q^m}^\times$ ce qui donne k modulo d ;*
   (f) *on répète avec d'autres T jusqu'à ce que le ppcm des d obtenus est N ce qui détermine k modulo N.*
3. *Soit $E/\mathbb{F}_q$ une courbe supersingulière avec $a = 0$; montrer que si $P \in E(\mathbb{F}_q)$ est d'ordre N alors $E[N] \subset E(\mathbb{F}_{q^2})$.*

Exercice 4. — *Soit $p \equiv 2 \mod 3$ et E la courbe elliptique définie sur $\mathbb{F}_p$ dont une équation affine est $y^2 = x^3 + 1$.*

1. *Montrer que $E/\mathbb{F}_p$ est supersingulière, i.e. de cardinal $p + 1$.*
2. *Soit $\omega \in \mathbb{F}_{p^2}$ une racine cubique de l'unité. Montrer que l'application $\beta : (x, y) \mapsto (\omega x, y)$ définit un endomorphisme de $E(\mathbb{F}_{p^2})$ en posant $\beta(O) = O$.*
3. *Soit $P \in E[n]$ de sorte que $\beta(P) \in E[n]$; on suppose que 3 ne divise pas n montrer alors que $e_n(P, \beta(P))$ est une racine primitive n-ème de l'unité.*
4. *En vous aidant de l'exercice précédent, résolvez le* ***problème de décision de Diffie-Hellmann*** *: connaissant P, aP, bP des points de $E(\mathbb{F}_q)$ et un point $Q \in \mathbb{F}_q$, peut-on déterminer si $Q = abP$?*
5. ***Protocole de Diffie-Hellmann tripartite*** *: soit P un point d'ordre n ; Alice, Bob et Chris choisissent des entiers secrets a, b, c modulo n respectivement et publient aP, bP et cP. Alice calcule $\tilde{e}_n(bP, cP)^a$, Bob $\tilde{e}_n(aP, cP)^b$ et Chris $\tilde{e}_n(aP, bP)^c$ ce qui constitue leur clef commune.*

Exercice 5. — *Pour factoriser 4453, considèrez la courbe elliptique d'équation*

1. $y^2 = x^3 + 10x - 2$ *modulo* 4453 *et* $P = (1, 3)$;
2. $y^2 = x^3 + 3x$ *modulo* 4453 *et* $P = (1, 2)$.

Exercice 6. — ***Test de primalité de Goldwasser-Kilian*** *: ce test n'est utilisé que pour des nombres ayant plus de* 100 *chiffres et ayant passé un grand nombre de tests de pseudo-primalité de sorte que l'on peut travailler avec* n *comme s'il était premier, i.e. comme si tous les nombres non divisibles par zéro qui apparaissent dans les calculs, sont inversibles (sinon on aurait un diviseur).*

1. *Soit* E *une courbe elliptique sur* $\mathbb{Z}/n\mathbb{Z}$ *; soient un entier* m *et* $P \in E(\mathbb{Z}/n\mathbb{Z})$ *satisfaisant les propriétés suivantes :*
   - *il existe un nombre premier* q *divisant* m *tel que* $q > (\sqrt[4]{n} + 1)^2$ *;*
   - $mP = O$ *;*
   - $(m/q)P = (x : y : t)$ *avec* $t \in (\mathbb{Z}/n\mathbb{Z})^\times$.

   Montrer alors que n *est premier.*
2. *Soient* $l_1, \cdots, l_k$ *des nombres premiers et des points finis* $P_i \in E(\mathbb{Z}/n\mathbb{Z})$ *tels que :*
   - $l_i P_i = O$ *pour tout* $1 \leq i \leq k$ *;*
   - $\prod_{i=1}^{k} l_i > (\sqrt[4]{n} + 1)^2$.

   Alors n *est premier.*
3. *Soit* n *premier avec* 6 *et* $m = \sharp E(\mathbb{Z}/n\mathbb{Z})$. *Montrer que s'il existe un nombre premier* $q | m$ *tel que* $q > (\sqrt[4]{n}+1)^2$ *alors il existe* $P \in E(\mathbb{Z}/n\mathbb{Z})$ *tel que* $mP = O$ *et* $(m/q)P = (x : y : t)$ *avec* $t \in (\mathbb{Z}/n\mathbb{Z})^\times$.
4. *On calcule le cardinal de* $E(\mathbb{Z}/n\mathbb{Z})$ *en utilisant par exemple l'algorithme de Schoof. Le principe de l'algorithme de Goldwasser-Kilian est le suivant. On essaye de diviser* m *par de petits premiers en espérant que le quotient* q *soit un nombre pseudo-premier plus grand que* $(\sqrt[4]{n} + 1)^2$. *Dans ce cas on suppose* q *premier et on cherche un point* $P \in E(\mathbb{Z}/n\mathbb{Z})$ *qui satisfait les hypothèses de la première question. Si un tel point* P *est trouvé, il nous faut prouver que* q *est bien premier : on utilise alors l'algorithme récursivement. Puisque* $q \leq m/2 \leq (n + 2\sqrt{n} + 1)/2$, *les nombres testés diminuent au moins de moitié à chaque itération de sorte que le nombre d'itération est* $O(\log n)$ *l'algorithme s'arrêtant dès que les nombres à tester deviennent assez petit pour employer d'autres tests.*

   Par exemple pour $n = 907$ *et* $E : y^2 = x^3 + 10x - 2$, *le point* $P = (819, 784)$ *vérifie* $71P = O$ *et comme* $71 > (907^{1/4} + 1)^2 \simeq 42.1$, *on déduit que* 907 *est premier, après avoir vérifié que* 71 *est premier.*

Exercice 7. — *Soit* E *la courbe elliptique* $y^2 + y = x^3 - x$ *sur le corps* $\mathbb{F}_p$ *avec* $p = 751$ *qui est de cardinal* $N = 727$. *On convient que les messages sont constitués des chiffres* $0 - 9$ *et des lettres* $A - Z$ *codés de* 10 *à* 35. *On utilise le cryptosystème du log discret avec* $\kappa = 20$.

1. *Comment codez-vous le message* « *STOP007* » *?*
2. *Traduisez le message reçu* $(361, 383)$, $(241, 605)$, $(201, 380)$, $(461, 467)$, $(581, 395)$.
3. *On utilise l'analogue du processus d'El Gamal ; avec la clef publique* $(201, 380)$ *et la suite aléatoire d'entiers* 386, 209, 118, 589, 312, 483, 335 *comment codez vous le message (1) ci-dessus ?*

1. Solutions

1 1) Le discriminant de E est 4 (modulo $11\mathbb{Z}$), il est non nul, donc E est une courbe elliptique définie sur $\mathbb{F}_{11}$. 2) Soit N l'ordre du groupe $E(\mathbb{F}_{11})$. Pour tout $z \in \mathbb{F}_{11}$, notons $\chi(z) = \left(\frac{z}{11}\right)$ le symbole de Legendre (cf. l'exercice 1). On a l'égalité

$$N = 1 + \sum_{x \in \mathbb{F}_{11}} \big(1 + \chi(x^3 + x + 6)\big). \tag{1}$$

Pour tout $x \in \mathbb{F}_{11}$, on détermine $\chi(x^3 + x + 6)$. Pour cela, on vérifie d'abord que l'ensemble des carrés de $\mathbb{F}_{11}$ (qui est de cardinal 6) est $\Big\{0, 1, 3, 4, 5, 9\Big\}$. Il en résulte que l'ensemble des couples $\big(x, \chi(x^3 + x + 6)\big)$ pour x parcourant $\mathbb{F}_{11}$ est

$$\Big\{(0,-1), (1,-1), (2,1), (3,1), (4,-1), (5,1), (6,-1), (7,1), (8,1), (9,-1), (10,1)\Big\}.$$

D'après l'égalité (1), on a donc $N = 13$. En notant O le point à l'infini de E, on en déduit par ailleurs que l'on a

$$E(\mathbb{F}_{11}) = \Big\{O, (2, \pm 4), (3, \pm 5), (5, \pm 2), (7, \pm 2), (8, \pm 3), (10, \pm 2)\Big\}.$$

3) La clé publique d'Alice est le point $K_A = 7P$. Afin de calculer les coordonnées de K_A, on utilise les égalités $K_A = P + 2P + 4P = P + 2P + 2(2P)$. On vérifie que l'on a

$$2P = (5, 2), \quad 4P = (10, 2), \quad 6P = (7, 9) \quad \text{et} \quad K_A = (7, 2).$$

4) Conformément au cryptosystème utilisé, Bob calcule les points

$$C_1 = 6P \quad \text{et} \quad 6K_A = (x, y).$$

On a $6K_A = 42P = 3P$, d'où $6K_A = (8, 3)$, d'où $x = 8$ et $y = 3$. Ensuite, Bob calcule le couple

$$C_2 = (9x, y) = (6, 3) \in \mathbb{F}_{11} \times \mathbb{F}_{11}.$$

Il envoie alors à Alice le couple $(C_1, C_2) = \Big((7, 9), (6, 3)\Big)$. Alice retouve le message M en procédant comme suit. Avec sa clé secrète, elle calcule le point $7C_1 = 6K_A$, ce qui lui permet de déterminer le couple (x, y). En utilisant C_2, elle en déduit M vu que l'on a $M = (8^{-1}6, 3^{-1}3)$ et que $8^{-1} = 7$.

2 D'après le théorème de Hasse, G est de cardinal au plus 54 de sorte que $m = 8$. Les points iP pour $1 \leq i \leq 7$ sont

$$(0, 1),\ (1, 39),\ (8, 23),\ (38, 38),\ (23, 23),\ (20, 28),\ (26, 9).$$

On calcule alors $Q - jmP$ pour $j = 0, 1, 2$ ce qui donne

$$(30, 40),\ (9, 25),\ (26, 9),$$

et on s'arrête car on retrouve P_7. On obtient alors $Q = (7 + 2\mu.8)P = 23P$.

3 1) Si $Q = kp$ alors $NQ = kNP = 0$ et $e_N(P, Q) = e_N(P, P)^k = 1^k = 1$. Réciproquement si $NQ = O$ alors $Q \in E[N]$ et comme $N \wedge q = 1$, on a $E|N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$. On choisit R tel que (P, R) est une base de $E[N]$ et alors $Q = aP = bR$ avec $e_N(P, R) = \zeta$ une racine primitive N-ième de l'unité. Ainsi si $e_N(P, Q) = 1$, on a

$$1 = e_N(P, Q) = e_N(P, P)^a e_N(P, R)^b = \zeta^b$$

de sorte que $b \equiv 0 \mod N$ et $bR = O$ et donc $Q = aP$.

2)

3) L'endomorphisme de Frobenius ϕ_q vérifie $\phi_q^2 - a\phi_q + q = 0$ et comme $a = 0$ alors $\phi_q^2 = -q$. Soit $S \in E[N]$; comme $E(\mathbb{F}_q)$ est de cardinal $q + 1$ et comme il existe un point d'ordre N, on a $N|q + 1$ soit $-q \equiv 1 \mod N$ et donc $\Phi_q^2(S) = -qS = 1.S$ d'où le résultat

4 1) cf. l'exercice 4 de la feuille 7.

2) L'image $\beta(E(\mathbb{F}_{p^2}))$ est clairement contenue dans $E(\mathbb{F}_{p^2})$; par ailleurs comme $(x, y) \mapsto (\omega^{-1}x, y)$ est inverse de β, on a égalité. On vérifie aussi que c'est un morphisme (via les formules d'addition...)

3) Le résultat découle directement du fait que P et $\beta(P)$ forment une base de $E[n]$, ce que nous allons prouver. Soient u, v des entiers tels que $uP = v\beta(P)$ alors $\beta(vP) = v\beta(P) = uP$. Si $vP = O$ alors $uP = O$ et donc $u \equiv 0$

mod n. Si $vP \neq O$ écrivons $vP = (x, y)$ avec $x, y \in \mathbb{F}_q$ alors $(\omega x, y) = \beta(vP) \in E(\mathbb{F}_q)$. Puisque $\omega \notin \mathbb{F}_q$ nous devons avoir $x = 0$ et ainsi $vP = (0, \pm\sqrt{b})$ qui est d'ordre 3 ce qui est impossible puisque par hypothèse 3 ne divise pas n.

4) On utilise l'accouplement de Weil, cf. l'exercice précédent, pour vérifier que Q est un multiple de P, i.e. si $e_n(P, Q) = 1$. Dans ce cas $Q = tP$ et on pose $\tilde{e}_n(P_1, P_2) = e_n(P_1, \beta(P_2))$ de sorte que

$$\tilde{e}_n(aP, bP) = \tilde{e}_n(P, P)^{ab} = \tilde{e}_n(P, abP) \text{ et } \tilde{e}_n(Q, P) = \tilde{e}_n(P, P)^t.$$

Si 3 ne divise pas n, alors $\tilde{e}_n(P, P)$ est une racine primitive n-ème de l'unité et donc

$$Q = abP \Leftrightarrow t \equiv ab \mod n \Leftrightarrow \tilde{e}_n(aP, bP) = \tilde{e}_n(Q, P).$$

5 1) On calcule $2P$: la pente de la tangente en P est

$$\frac{3x^2 + 10}{2y} = \frac{13}{6} \equiv 3713 \mod 4453.$$

Comme $6 \wedge 4453 = 1$, on calcule $6^{-1} \equiv 3711 \mod 4453$ et donc $2P = (x, y)$ avec

$$x \equiv 3713^2 - 2 \equiv 4432, \quad y \equiv -3713(x - 1) - 3 \equiv 3230.$$

On calcule $3P = P + 2P$: la pente est

$$\frac{3230 - 3}{4332 - 1} = \frac{3227}{4331}.$$

Comme $4331 \wedge 4453 = 61 \neq 1$ ce qui ne permet pas d'évaluer la pente mais fournit un diviseur 61 de $4453 = 61.73$.

2) On calcule $2P$; la pente de la tangente en P est

$$\frac{3x^2 + 3}{2y} = \frac{3}{2} \equiv 2228 \mod 4453.$$

Comme $2 \wedge 4453 = 1$, on calcule $2^{-1} \equiv 2227 \mod 4453$ et donc $2P = (x, y)$ avec

$$x \equiv 3340 \mod 4453, \quad y \equiv 1669 \mod 4453.$$

On calcule $3P = 2P + P$; la pente est

$$\frac{1669 - 2}{3340 - 1} \equiv 746 \mod 4453.$$

Comme $3339 \wedge 4453 = 1$, on calcule $3339^{-1} \equiv 1483 \mod 4453$. On obtient alors $3P = (x, y)$ avec

$$x \equiv 1003 \mod 4453, \quad y \equiv 610 \mod 4453.$$

On calcule ensuite $6P = 3P + 3P$; le dénominateur de la pente est $2.610 = 1220$ et nous voyons que $1220 \wedge 4453 = 61$.

6 1) Soit p un facteur premier de n ; en réduisant modulo p, l'image de P a un ordre divisant m mais ne divisant pas m/q puisque $t \in (\mathbb{Z}/n\mathbb{Z})^\times$. Puisque q est premier il divise l'ordre de l'image de P dans $E(\mathbb{F}_p)$ et donc ce dernier est de cardinal supérieur ou égal à q et donc, d'après le théorème de Hasse $q \leq (\sqrt{p} + 1)^2$. Ainsi pour $p \leq \sqrt{n}$, on obtient $q \leq (\sqrt[4]{n} + 1)^2$ d'où contradiction.

2) Soit p premier divisant $n = p^f n_1$ avec $p \wedge n_1 = 1$ alors $E(\mathbb{Z}/n\mathbb{Z}) = E(\mathbb{Z}/p^f\mathbb{Z}) \oplus E(\mathbb{Z}/n_1\mathbb{Z})$. La réduction modulo p de P_i est alors d'ordre l_i et donc l_i divise le cardinal de $E(\mathbb{F}_p)$ soit

$$(\sqrt[4]{n} + 1)^2 < \prod_{i=1}^{k} l_i \leq \sharp E(\mathbb{F}_p) < p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2,$$

et donc $p > \sqrt{n}$ et donc n premier.

3) Posons $G = E(\mathbb{Z}/n\mathbb{Z})$; supposons que pour tout $P \in G$ nous avons $(m/q)P = O$ alors $G \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$ avec $d_2 | d_1$ avec $m = d_1 d_2 \leq d_1^2 \leq (m/q)^2$ et donc $q^2 \leq m$. Utilisant notre hypothèse sur la taille de q et le théorème de Hasse, nous avons $(\sqrt[4]{n} + 1)^2 < \sqrt{n} + 1$ ce qui est absurde.

7 (1) Le message envoyé est $(562, 576)$, $(581, 395)$, $(484, 214)$, $(501, 220)$, $(1, 0)$, $(1, 0)$, $(144, 565)$.

(2) ICANT

(3) $(676, 182)$, $(385, 703)$, $(595, 454)$, $(212, 625)$, $(261, 87)$, $(77, 369)$, $(126, 100)$, $(66, 589)$, $(551, 606)$, $(501, 530)$, $(97, 91)$, $(733, 110)$, $(63, 313)$, $(380, 530)$.