Examen de Cryptologie

18 juin mai 2021
Durée 1h30

Auteurs
Jérémy Berthomieu & Valérie Ménissier-Morain

Version du 17 juin 2021

Le seul document autorisé est une feuille manuscrite A4 recto-verso.
L'utilisation d'un appareil électronique est proscrit pendant toute la durée de l'épreuve.
La note finale est le minimum entre 20 *et la somme des points obtenus sur* 28*. Le barème est indicatif.*

Exercice 1 – Questions – 4 points

1. (**Générateur – 2 points**) Si a et n sont premiers entre eux montrez que a est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$. Est-ce le cas dans $(\mathbb{Z}/n\mathbb{Z}, *)$? Si oui démontrez-le, si non donnez un contre-exemple.

> **Solution :**
> a est générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$ si pour tout $b \in \mathbb{Z}/n\mathbb{Z}$, il existe un témoin $k \in \mathbb{Z}/n\mathbb{Z}$ tel que $ak = b \bmod n$.
> Comme a est premier avec n, il existe un couple d'entiers (u, v) tel que $au+nv = 1$ (relation de Bezout) soit $au = 1 \bmod n$.
> Soit $b \in \mathbb{Z}/n\mathbb{Z}$. En multipliant l'identité précédente par b on obtient $aub = b \bmod n$ donc $k := ub \bmod n$ est un témoin pour b et a est bien générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$.
>
> Cela n'est pas vrai pour la multiplication ! Par exemple 2 et 7 sont premiers entre eux mais 2 n'est pas générateur de $(\mathbb{Z}/7\mathbb{Z}, *)$. En effet, le sous-groupe engendré par 2 est $\{2, 4, 1\}$. Or le cardinal de $(\mathbb{Z}/7\mathbb{Z}, *)$ est $\varphi(7) = 6$ car 7 est premier.

2. (**RSA – 2 points**) a. Donner les relations qui lient les différents paramètres utilisés dans RSA.

> **Solution :**
> Les paramètres de RSA sont
> — deux nombres premiers distincts p et q ;
> — un entier $n = pq$;
> — l'indicatrice d'Euler de n, $\varphi(n) = n - p - q + 1$;
> — un entier d premier avec $\varphi(n)$ et son inverse e modulo $\varphi(n)$.

b. Parmi ces paramètres, lesquels sont publics et lesquels restent secrets ?

> **Solution :**
> La clef publique est constituée de n et e.
> La clef privée est constituée de p, q, d et $\varphi(n)$.

Exercice 2 – DLP – 6,5 points

Dans cet exercice, la méthode de résolution est laissée au choix. En revanche, elle doit être expliquée et tous les calculs doivent être justifiés.

On considère le groupe $(\mathbb{Z}/409\mathbb{Z}, +)$ et son générateur $g = 229$. Soit $h = 345$, donner le logarithme discret de h dans la base g.

Solution :

Version groupe additif avec Euclide étendu On est dans un groupe cyclique additif, il suffit donc de calculer l'inverse g^{-1} mod 409 de g avec l'algorithme d'Euclide étendu appelé sur 409 et g. Ensuite, on multiplie h et g^{-1} pour en déduire le logarithme discret de h en base g.

Cela nous donne les calculs suivants

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
-1				409	1	0
0			409	229	0	1
1	409	1	229	180	1	-1
2	229	1	180	49	-1	2
3	180	3	49	33	4	-7
4	49	1	33	16	-5	9
5	33	2	16	1	14	-25
6	16	16	1	0	-229	409

À l'avant-dernière ligne, il y a un 1 dans la cinquième colonne donc le pgcd de 409 et 229 est 1, 229 est premier avec 409 donc inversible modulo 409 d'inverse le cofacteur de 229 sur cette ligne $v_6 = -25$.

Ici il n'est pas nécessaire de calculer la suite des u_i le cofacteur associé à 409 ni de calculer la dernière ligne qui ne sert que de vérification.

Enfin, on calcule $-25 \times h = -25 \times 345 \bmod 409 = (-25) \times (-64) \bmod 409 = 1600 \bmod 409 = 373$. Donc le logarithme discret de h en base g est 373.

Version groupe additif avec Baby-step Giant-step Le groupe est d'ordre $n = 409$ donc on prend $s = \lfloor \sqrt{n} \rfloor + 1 = 21$.

On calcule les pas de bébés $(j, g \times j \bmod 409)$ pour $j = 0, \ldots, 20$.

$(0,0), (1,229), (2,49), (3,278), (4,98), (5,327), (6,147), (7,376), (8,196), (9,16),$
$(10,245), (11,65), (12,294), (13,114), (14,343), (15,163), (16,392), (17,212), (18,32), (19,261),$
$(20,81)$.

On calcule les pas de géants $(j, h - g \times s \times j \bmod 409) = (j, h - 310j \bmod 409)$ pour $j = 0, \ldots, 21$.

$(0,345), (1,35), (2,134), (3,233), (4,332), (5,22), (6,121), (7,220), (8,319), (9,9),$
$(10,108), (11,207), (12,306), (13,405), (14,95), (15,194), (16,293), (17,392), (18,82), (19,181),$
$(20,280)$.

On remarque qu'il y a une collision en $(16, 392)$, pour les pas de bébés, et $(17, 392)$, pour les pas de géants. Donc le logarithme discret de h en base g est $16 + 17 \times s = 16 + 17 \times 21 = 373$.

Version groupe multiplicatif avec Baby-step Giant-step *Cette "correction" ne convient pas, elle n'est là que pour suivre les calculs d'un étudiant qui aurait répondu dans le groupe multiplicatif !*

Le groupe est d'ordre $n = 408$ donc on prend $s = \lfloor \sqrt{n} \rfloor + 1 = 21$.

On calcule les pas de bébés $(j, g^j \bmod 409)$ pour $j = 0, \ldots, 20$.

$(0,1), (1,229), (2,89), (3,340), (4,150), (5,403), (6,262), (7,284), (8,5), (9,327),$
$(10,36), (11,64), (12,341), (13,379), (14,83), (15,193), (16,25), (17,408), (18,180), (19,320),$
$(20,69)$.

On calcule les pas de géants $(j, h \times g^{-sj} \bmod 1009$ pour $j = 0, \ldots, 20$.

$(0, 345), (1, 284), (2, 69), (3, 384), (4, 341), (5, 404), (6, 150), (7, 408), (8, 30), (9, 327)$,
$(10, 6), (11, 229), (12, 83), (13, 373), (14, 262), (15, 320), (16, 216), (17, 64), (18, 125), (19, 340)$,
$(20, 25)$.

On remarque qu'il y a une collision en $(9, 327)$, pour les pas de bébés les pas de géants. Donc le logarithme discret de h en base g est $9 + 21 \times s = 9 + 9 \times 21 = 198$.

Exercice 3 – Courbes Elliptiques – 12,5 points

Dans cet exercice, on s'intéresse au groupe additif E défini à partir des points rationnels de la courbe elliptique définie par l'équation $y^2 = x^3 + 2x$ sur $\mathbb{F}_{17}$.

1. (**1 point**) Justifier que cette courbe est bien elliptique.

Solution :

La courbe est d'équation $y^2 = x^3 + ax + b$ définie sur $\mathbb{F}_{17}$ avec $a = 2$ et $b = 0$. Elle semble donc elliptique.

Elle est elliptique si, et seulement si, $\Delta = 16(4a^3 + 27b^2) \neq 0$. Or $4a^3 + 27b^2 = 4 \times 8 + 0 = 32 \neq 0$ et $\Delta \neq 0$.

2. (**1 point**) Donner l'ensemble des carrés dans $\mathbb{F}_{17}$.

Solution :

y	y^2
0	0
± 1	1
± 2	4
± 3	9
± 4	16
± 5	8
± 6	2
± 7	15
± 8	13

3. (**3 points**) Donner, sous la forme d'un tableau comme vu en cours/TD, l'ensemble des points rationnels définissant E. Montrer que E est de cardinal 20.

Solution :

x	$x^3 + 2x$	Point(s)
0	0	$(0, 0)$
1	3	
2	12	
3	16	$(3, \pm 4)$
4	4	$(4, \pm 2)$
5	16	$(5, \pm 4)$
6	7	
7	0	$(7, 0)$
8	1	$(8, \pm 1)$
9	16	$(9, \pm 4)$
10	0	$(10, 0)$
11	10	
12	1	$(12, \pm 1)$
13	13	$(13, \pm 8)$
14	1	$(14, \pm 1)$
15	5	
16	14	

Il y a donc trois points d'ordre 2 sur l'axe des abscisses : $(0,0)$, $(7,0)$ et $(10,0)$ plus 8 paires de points symétriques, ce qui donne 19 points rationnels. Il faut rajouter à tout cela le point à l'infini,on obtient donc 20 points.

4. (**1 point**) À l'aide du théorème de structure, montrer que soit $(E,+) \simeq (\mathbb{Z}/20\mathbb{Z},+)$, soit $(E,+) \simeq (\mathbb{Z}/2\mathbb{Z}\times \mathbb{Z}/10\mathbb{Z},+)$.

Solution :
Le groupe $(E,+)$ est d'ordre 20 donc il est isomorphe soit à $(\mathbb{Z}/20\mathbb{Z},+)$ soit, par le théorème de structure à $(\mathbb{Z}/d_1\mathbb{Z}\times\mathbb{Z}/d_2\mathbb{Z},+)$ avec $d_1 \mid (p-1)$, $d_1 \mid d_2$ et $d_1 d_2 = 20$.
Comme $p-1 = 16$ et le pgcd de 16 et 20 est 4, on peut avoir
— $d_1 = 2$ et $d_2 = 10$;
— $d_1 = 4$ et $d_2 = 5$ mais alors d_1 ne divise pas d_2.
Ainsi $(E,+)$ est isomorphe à $(\mathbb{Z}/20\mathbb{Z},+)$ ou $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z},+)$.
Puisque E a trois points d'ordre 2, alors il ne peut être cyclique. Ainsi, on peut déjà conclure qu'il s'agit du second cas. Voir aussi question plus bas.

5. (**1 point**) Montrer que dans $(\mathbb{Z}/20\mathbb{Z},+)$, il n'existe qu'un seul élément $h \neq 0$ tel que $[2]h = 0$. En déduire que $(E,+) \not\simeq (\mathbb{Z}/20\mathbb{Z},+)$.

Solution :
Si $[2]h = 0 \bmod 20$, alors $2h = 20k$, $k \in \mathbb{Z}$ et $h = 10k$. Ainsi, modulo 20, $h = 0$ ou $h = 10$ et 10 le seul non nul.
Comme dans $\mathbb{Z}/20\mathbb{Z}$, il n'y a qu'un élément d'ordre 2 et que dans E, il y en a 3, on en déduit que $(E,+) \not\simeq (\mathbb{Z}/20\mathbb{Z},+)$.

6. (**0,5 point**) On souhaite maintenant trouver deux points P et Q de E qui engendrent ensemble E. Soit $P = (7,0)$ et $Q = (4,2)$; vérifier que ce sont bien deux points de E.

Solution :
On voit qu'il y a dans notre tableau le point $(7,0)$ et la paire $(4,\pm 2)$ donc $P = (7,0)$ et $Q = (4,2)$ sont bien des points de E.
Alternativement, $7^3 + 2\times 7 = (49+2)\times 7 = 0\times 7 = 0 \bmod 17$ et $4^3 + 2\times 4 - (2)^2 = 4^3 + 4 \bmod 17 = -4 + 4 = 0 \bmod 17$.

7. (**3 points**) Calculer $[5]Q$.

Solution :
On utilise la méthode du "double and add" (le "square and multiply" dans un groupe additif), c'est-à-dire que l'on calcule $[2]Q = Q + Q$, puis $[4]Q = [2]Q + [2]Q$ et enfin $[5]Q = [4]Q + Q$.
— On calcule tout d'abord $[2]Q = Q + Q = (x,y)$:
$\lambda = \frac{3x_Q^2+2}{2y_Q} = \frac{3\times 16+2}{4} = \frac{-1}{4} = -1\times(-4) = 4 \bmod 17$ donc
• $x = \lambda^2 - x_Q - x_Q = 4^2 - 4 - 4 = 8 \bmod 17$;
• $y = \lambda(x_Q - x) - y_Q = 4\times(4-8) - 2 = 1 - 2 = -1 = 16 \bmod 17$.
$[2]Q = (8,16)$.
— Pour information, si l'étudiant a calculé $[3]Q = [2]Q + Q$, alors le résultat est $[3]Q = (13,9)$.
— On calcule ensuite $[4]Q = [2]Q + [2]Q = (x,y)$:
$\lambda = \frac{3x_{[2]Q}^2+2}{2y_{[2]Q}} = \frac{3\times 64+2}{1} = 3\times 13 = 5 \bmod 17$ donc

- $x = \lambda^2 - x_{[2]Q} - x_{[2]Q} = 5^2 - 8 - 8 = 9 \bmod 17$;
- $y = \lambda(x_{[2]Q} - x) - y_{[2]Q} = 5 \times (8 - 9) - 16 = -5 - 16 = -21 = 13 \bmod 17$.

$[4]Q = [9, 13]$.

— On calcule enfin $[5]Q = [4]Q + Q = (x, y)$:
$\lambda = \frac{y_{[4]Q} - y_Q}{x_{[4]Q} - x_Q} = \frac{13-2}{9-4} = \frac{11}{5} = 11 \times 7 = 77 = 9 \bmod 17$ donc

- $x = \lambda^2 - x_{[4]Q} - x_Q = 9^2 - 9 - 4 = 68 = 0 \bmod 17$;
- $y = \lambda(x_{[4]Q} - x) - y_{[4]Q} = 9 \times (9 - 0) - 13 = 68 = 0 \bmod 17$.

$[5]Q = (0, 0)$.

8. (**0,5 point**) En déduire que Q est d'ordre 10.

Solution :
Comme $E \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, alors par le théorème de Lagrange, les ordres possibles des éléments sont les diviseurs de 10 : 1, 2, 5 ou 10.
Clairement $Q \neq \mathcal{O}$ donc il n'est pas d'ordre 1. De plus, $y_Q \neq 0$ et on a calculé $[2]Q = (8, 16) \neq \mathcal{O}$ donc il n'est pas d'ordre 2 non plus. De même, $[5]Q = (0, 0) \neq \mathcal{O}$ donc il n'est pas d'ordre 5 non plus. Ainsi, il est d'ordre 10 (ce qui concordre avec le fait que $[5]Q$ est d'ordre 2).

9. (**1 point**) On considère l'ensemble F des éléments de E qui s'écrivent sous la forme $[i]P + [j]Q$ avec $(i, j) \in \{0, 1\} \times \{0, 1, \ldots, 9\}$. Montrer que F est un sous-groupe de E d'ordre supérieur ou égal à 11.

Solution :
Par définition, le neutre, $\mathcal{O} = [0]P + [0]Q$, est dans F.
Si $R = [i]\,P \circ [j]\,Q$ et $S = [k]\,P \circ [\ell]\,Q$ sont dans F, alors $R + S = [i]\,P + [j]\,Q + [k]\,P + [\ell]\,Q = [i]\,P + [k]\,P + [j]\,Q + [\ell]\,Q = [i + k]\,P + [j + \ell]\,Q$.
Or, P est d'ordre 2 donc $i + k$ peut être réduit modulo 2 et de même Q est d'ordre 10 donc $j + \ell$ peut être réduit modulo 10. Ainsi, $R + S \in F$.
L'inverse de R est S tel que $i + k = 0 \bmod 2$ et $j + \ell = 0 \bmod 10$, c'est-à-dire $k = 2 - i \bmod 2 = i$ et $\ell = 10 - j \bmod 10$ donc $S \in F$.
Enfin, F contient tout le sous-groupe engendré par Q, c'est-à-dire au moins 10 éléments distincts de P, et P donc au moins 11 éléments distincts.

10. (**0,5 point**) En déduire que $F = E$.

Solution :
Par le théorème de Lagrange, $|F|$ divise $|E| = 20$. Or, $|F| \geq 11$ donc $|F| = 20$ et $F = E$.

Exercice 4 – Nouvelles du front – 5 points

Vauban envoie des nouvelles du siège de Lille au roi de France. Il chiffre son message avec le système de chiffrement de Vigenère :

```
NCEVMXSXPWBPDOGMTWWGPWBCWBOYMLMPZYBOWBPYNUGICWTTDZPIAESBZYDPSIQVIYUOTWMGSIMEV
```

Que lui dit-il ?

La démarche, même inaboutie, est plus importante que la teneur du message lui-même.

Solution :
Les techniques usuelles (détermination de la longueur de la clef par test de Kasiski ou indice de coïncidence) ne marchent pas sur un texte aussi bref.

On va donc utiliser les informations claires probables :

— expéditeur : `Vauban`
— destinataire : `roi`, `sire`, `Votre Majesté`,
— lieu `Lille`, `ville`, `siège`, `citadelle`
— etc.

en les cherchant au début ou à la fin du message , en espérant que la clef n'est pas plus longue . Pour la plupart de ces mots s'ils sont présents dans le message il est difficile de les localiser donc d'exploiter l'information. Mais le mot le plus probable est `VAUBAN` en signature donc à la fin du message.

Si on suppose que la clef est de longueur 6 (la longueur du mot `VAUBAN`), on écrit le texte sur 6 colonnes, ce qui donne :

```
NCEVM
XSXPWB
PDOGMT
WWGPWB
CWBOYM
LMPZYB
OWBPYN
UGICWT
TDZPIA
ESBZYD
PSIQVI
YUOTWM
GSIMEV
```

et la dernière ligne `GSIMEV` serait le chiffré probable de `VAUBAN`, on déduit que la clef est

```
  GSIMEV
- VAUBAN
--------
= SOLEIL
```

Cela paraît particulièrement prometteur puisque la clef serait un mot, donc facile à retenir et partager. On essaie de déchiffrer le reste avec la clef `SOLEIL`, ce qui donne :

```
VOTRE
MAJEST
ELAVIL
LESEST
RENDUE
AUBOUT
DENEUF
JOURSL
ILLEES
TANOUV
EAUFRA
NCAISE
VAUBAN
```

autrement dit

```
Votre majesté, la ville s'est rendue au bout de neuf jours.
Lille est à nouveau française. Vauban
```

Le message est bien déchiffré. On constate que `Lille` et `ville` font bien partie du message mais ne sont pas placés de façon aussi favorable que `Vauban` pour la cryptanalyse.