Examen de Cryptologie

11 mai 2021
Durée 1h30

Auteurs
Jérémy Berthomieu, Valérie Ménissier-Morain & Clara Pernot

Version du 30 mai 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* 30.

Exercice 1 – Questions – 4 points

1. (**1 point**) On note $p > 2$ un nombre premier.
   Parmi les réponses suivantes, dire lequelles sont correctes en justifiant.
   La réciprocité quadratique permet de
   (a) savoir si -1 est un carré modulo p.
   (b) déterminer une racine carrée de 2 modulo p.
   (c) savoir que $q > 2$, un nombre premier, est un carré modulo p si, et seulement si, p est un carré modulo q.
   (d) savoir si $q > 2$, un nombre premier, est un carré modulo p suivant si p est un carré modulo q.

   Solution :
   (a) En effet, c'est le cas si, et seulement si, $p = 1 \bmod 4$.
   (b) indique seulement si une racine carrée existe mais ne permet pas d'en calculer une
   (c) ce n'est pas inconditionnel comme le montre la réponse pour la dernière proposition
   (d) Si $p = 1 \bmod 4$ ou $q = 1 \bmod 4$, alors $(\frac{p}{q}) = (\frac{q}{p})$, sinon, $(\frac{p}{q}) = -(\frac{q}{p})$.
   La différence entre les deux dernières propositions est dans le premier cas si et seulement si *qui corresponda à une équivalence, alors que dans le second cas* suivant si *indique un lien beaucoup moins fort.*

2. (**1 point**) Soient a et b deux entiers non nuls. Montrer que $\frac{a}{b} = [q_1, q_2, \ldots, q_r] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \frac{1}{q_r}}}$ où $q_1, q_2, \ldots, q_r$ sont les quotients apparaissant dans l'algorithme d'Euclide appelé avec a et b.

Solution :
Notons $r_0 = a$, $r_1 = b$ et $r_0 = q_1 r_1 + r_2$. On a alors $\frac{a}{b} = \frac{r_0}{r_1} = q_1 + \frac{r_2}{r_1} = q_1 + \frac{1}{\frac{r_1}{r_2}}$ et on rappelle récursivement sur r_1 et r_2. On s'arrête quand $r_n = 0$.
Pour faire une récurrence propre sur r, on prend comme propriété : pour tout couple d'entiers (a, b) pour lesquels l'algorithme d'Euclide produit r quotients successifs $q_1, \ldots, q_r$, on a $\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \frac{1}{q_r}}}$.

3. (**1 point**) Montrer que le DLP se résout en temps polynomial dans $(\mathbb{Z}/n\mathbb{Z}, +)$.

Solution :
Soit g un générateur et h l'élément dont on veut le logarithme discret. On cherche donc t tel que $h = [t]g \bmod n$. Comme g est un générateur, il suffit de connaître son inverse modulo n, ce qui se calcule en temps $O((\log n)^2)$ opérations, puis de multiplier cet inverse par h en temps $O((\log n)^2)$ opérations.
Une erreur commune est de faire appel à l'algorithme Baby Step Giant Step en toute confiance puisque c'est algorithme est optimal dans le cas général. Dans ces conditions la complexité est en $\sqrt{n} = 2^{\log(n)/2}$ donc est un algorithme exponentiel. Ici il s'agit d'un groupe précis, pour lequel on a un algorithme moins goourmand.

4. (**1 point**) Donner une attaque par canaux auxiliaires sur RSA et un moyen de prévenir cette attaque.

Solution :
Par exemple
- Attaque de Kocher avec un oscilloscoque afin de déterminer les multiplications effectuées lorsqu'un bit de la clef secrète vaut 1.
  On peut prévenir cette attaque en effectuant les multiplications quelle que soit la valeur du bit de la clef secrète, on garde ou non le résultat.
- Attaque par faute sur RSA+CRT : on introduit une faute lors du déchiffrement modulo un seul des deux premiers. On obtient alors un message déchiffré erroné. La différence entre le clair et le déchiffré erroné est un multiple de l'autre premier et un pgcd avec n permet de retrouver cet autre premier.
  On peut prévenir cette attaque en demandant à la machine de vérifier que le chiffré du message déchiffré est bien celui donné à l'origine. Si c'est le cas, elle retourne le déchiffré, sinon elle recommence ses calculs de déchiffrement.

Exercice 2 – RSA – 8 points

Les 2 parties de l'exercice sont indépendantes.

Alice et Bob souhaitent communiquer en utilisant RSA. Alice crée donc une paire de clefs dont la clef publique est (n, e).

On s'intéresse à 2 scénarios.

1. (**Alice est naïve – 2,5 point**) Oscar a intercepté un chiffré $c = m^e \bmod n$. Dans un jour de gentillesse, Alice accepte de déchiffrer un message c' qu'Oscar choisirait si, seulement si, $c' \neq c$.
   Oscar calcule $c' = 2^e c \bmod n$.
   (a) (1 point) Si $c' = c$, montrer comment Oscar peut retrouver m.

Solution :
Si $c' = c$, alors Alice refuse de déchiffrer c' (sinon puisqu'elle déchiffre c', elle déchiffre c et fournit directement m à Oscar).
Avec les informations dont il dispose, Oscar déduit que $c = c' = 2^e\, c \bmod n$, et en élevant les deux membres à la puissance d on obtient $c^d = 2^{e\,d} c^d \bmod n$. Or par définition $e\,d = 1 \bmod \varphi(n)$ donc il existe k tel que $e\,d = 1 + k\varphi(n)$. Puisque 2 est premier avec n, d'après le théorème d'Euler $2^{\varphi(n)} = 1 \bmod n$ donc $2^{e\,d} = 2^{1+k\varphi(n)} = 2 \bmod n$. Par conséquent $c^d = 2\, c^d \bmod n$, puisque $m = c^d$, on a $m = 2\, m \bmod n$ donc $m = 0 \bmod n$ et Oscar a trouvé la valeur de m sans l'aide d'Alice.

(b) (1,5 point) Si $c' \neq c$, montrer comment Oscar peut retrouver m.

Solution :
Comme dans la question précédente on a $c'^d = 2\, m \bmod n$. Ainsi, il faudra multiplier le déchiffré de c' par l'inverse de 2 modulo n, qui est $\frac{n+1}{2}$, pour obtenir le déchiffré de c.
Notons que cette astuce fonctionne pour 2 *ou n'importe quel autre entier inversible modulo* n.

2. (**Alice est amnésique – 5,5 points**) *Pour chacune des deux sous-questions, un raisonnement général est demandé avant d'effectuer les calculs correspondants.*
La clef publique d'Alice est $(n, e) = (20099, 11857)$.

(a) (2 points) Alice a oublié quels premiers p et q elle a utilisés pour obtenir n. Mais sa clef privée contient $\varphi(n) = 19800$. Retrouver p et q, sans recherche exhaustive, avec l'hypothèse que $p < q$.
On pourra utiliser le fait que $98^2 = 9604$.

Solution :
Le polynôme $(x-p)(x-q) = x^2 - (p+q)x + pq$ admet, par définition, p et q comme racines. Or, $pq = n = 20099$ et $\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$. Ainsi, $-(p+q) = \varphi(n) - n - 1 = 19800 - 20099 - 1 = -300$ et p et q sont les racines de

$$x^2 - (p+q) + pq = x^2 + (\varphi(n) - n - 1)x + n = x^2 - 300x + 20099.$$

On calcule donc ses racines avec $\Delta = (-300)^2 - 4 \times 20099 = 90000 - 80396 = 9604 = 98^2$. On a donc

$$p = \frac{300 - 98}{2} = \frac{202}{2} = 101, \quad q = \frac{300 + 98}{2} = \frac{398}{2} = 199.$$

(b) (3,5 points) Vérifier que le choix de e est correct et déterminer le reste de la clef privée.

Solution :
Pour que le choix de e soit correct, il faut que e soit inversible modulo $\varphi(n)$. De plus, le reste de la clef privée, d, est l'inverse de e modulo $\varphi(n)$.
Le calcul de l'inverse s'effectue en appelant l'algorithme d'Euclide étendu sur $\varphi(n)$ et e.
Le tableau suivant présente le calcul du pgcd de $a = \varphi(n) = 19800$ et $b = e = 11857$. Chaque ligne à partir de la ligne $i = 1$ se lit :
- pour la partie gauche (colorée en rose), si $r_i \neq 0$, la division euclidienne de r_{i-1} par r_i est $r_{i-1} = q_i * r_i + r_{i+1}$ qui définit le quotient $q_i = \lfloor \frac{r_{i-1}}{r_i} \rfloor$ et le reste suivant $r_{i+1} = r_{i-1} - q_i * r_i$; sinon on s'arrête.
- pour la partie droite (colorée en jaune), $u_{i+1} = u_{i-1} - q_i * u_i$ et $v_{i+1} = v_{i-1} - q_i * v_i$
- avec l'initialisation (partie en haut, colorée en bleu) : $r_0 = a$, $r_1 = b$, $u_0 = v_1 = 1$, $v_0 = u_1 = 0$
- à chaque étape on a $r_i = u_i\, a + v_i\, b \ \ \forall i$.

À l'avant-dernière ligne, on trouve dans la cinquième colonne le dernier reste positif, c'est-à-dire le pgcd de a et b.

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
-1					1	0
0			19800	11857	0	1
1	19800	1	11857	7943	1	-1
2	11857	1	7943	3914	-1	2
3	7943	2	3914	115	3	-5
4	3914	34	115	4	-103	172
5	115	28	4	3	2887	-4821
6	4	1	3	1	-2990	4993
7	3	3	1	0	11857	-19800

À l'avant-dernière ligne, il y a un 1 dans la cinquième colonne donc le pgcd de $\varphi(n)$ et e est 1, e est premier avec $\varphi(n)$ donc inversible modulo $\varphi(n)$ d'inverse le cofacteur de e sur cette ligne $v_7 = 4993$.

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

Exercice 3 – Courbes Elliptiques – 18 points

Dans tout 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 $\mathbb{F}_{257}$.

En utilisant aussi bien le représentant canonique $c \bmod n$ que $n - c$ pour réduire la taille des nombres manipulés, seuls des calculs donnant lieu à des nombres à 3 chiffres maximum sont à effectuer, hormis à la question 9 où une opération a un résultat à 4 chiffres, De plus, pour les calculs les plus complexes des indications sont fournies.

1. (**1 point**) Vérifier que 257 est bien premier.

Solution :
Il suffit de tester qu'il n'est pas divisible par les nombres premiers inférieurs à $\sqrt{257}$. Or $256 = 16^2$ donc il suffit de tester pour 2, 3, 5, 7, 11 et 13. Clairement, 2 et 5 ne divisent pas 257. Comme $2+5+7 = 14$, 3 ne divise pas 257 non plus. Si 7 le divisait, alors il diviserait $250 = 2 \times 5^3$ ce qui n'est pas vrai. Enfin $257 = 23 \times 11 + 4$ et $257 = 19 \times 13 + 10$ donc il est bien premier.

2. (**1 point**) Justifier que cette courbe est bien elliptique.

Solution :
La courbe est d'équation $y^2 = x^3 + ax + b$ définie sur $\mathbb{F}_{257}$ avec $a = 2$ et $b = 0$. Elle semble donc elliptique.
Elle est elliptique si, et seulement si, $\Delta = 16(4a^3 + 27b^3) \neq 0$. Or $4a^3 + 27b^2 = 4 \times 8 + 0 = 32 \neq 0$ et $\Delta \neq 0$.

3. (**2 points**) Déterminer, s'ils existent, les points d'abscisse 0 de E.
Calculer 68^2 dans $\mathbb{F}_{257}$. En déduire que E admet au moins trois points d'ordonnée 0 dont $(68, 0)$.

Solution :
On a $0^3 + 2 \times 0 = 0$ donc la courbe admet $(0, 0)$ comme unique point d'abscisse 0.
On a $68^2 = 68 \times 4 \times 17 = 272 \times 17 = 15 \times 17 = 255 = -2 \bmod 257$. Ainsi $(\pm 68)^3 + 2 \times (\pm 68) = \pm 68 \times (68^2 + 2) = 0 \bmod 257$ et la courbe admet aussi les points $(\pm 68, 0)$, c'est-à-dire $(68, 0)$ et $(257 - 68, 0) = (189, 0)$.
L'équation $x^3 + 2x = 0$ ne peut avoir au plus que trois solutions dans le corps $\mathbb{F}_{257}$. Puisqu'on en a déjà déterminé 3, à savoir 0, 68 et 189, la courbe admet exactement trois points d'ordonnée 0.

4. (**2 points**) Montrer que E admet deux points d'abscisse 4 si, et seulement si, 72 est un carré modulo 257. Puis déterminer si E possède de tels points.

Solution :
Comme $4^3 + 2 \times 4 = 64 + 8 = 72$, alors E a deux points $(4, \pm y)$ si, et seulement si, $y^2 = 72 \bmod 257$.
En utilisant le symbole de Legendre, on a $(\frac{72}{257}) = (\frac{36 \times 2}{257}) = (\frac{6^2}{257})(\frac{2}{257}) = (\frac{2}{257})$. Or $257 = 1 \bmod 8$ donc $(\frac{2}{257}) = 1$ et 72 est un carré modulo 257.

5. (**2 points**) Donner une condition nécessaire et suffisante pour que E admette deux points d'abscisse 8. Puis déterminer si E possède de tels points.

Solution :
Comme $8^3 + 2 \times 8 = 512 + 16 = -2 + 16 = 14$, alors E a deux points $(8, \pm y)$ si, et seulement si, $y^2 = 14 \bmod 257$. Autrement dit si, et seulement si, 14 est un carré modulo 257.
En utilisant le symbole de Legendre, on a $(\frac{14}{257}) = (\frac{2}{257})(\frac{7}{257})$ et $(\frac{2}{257}) = 1$ d'après la question précédente.
Comme $257 = 1 \bmod 4$, on a $(\frac{7}{257}) = (\frac{257}{7}) = (\frac{5}{7})$.
- Or les carrés non nuls modulo 7 sont 1, 2 et 4 donc $(\frac{5}{7}) = -1$ et 14 n'est pas un carré modulo 257 ;
- Comme $5 = 1 \bmod 4$, on a $(\frac{5}{7}) = (\frac{7}{5}) = (\frac{2}{5}) = -1$ et 14 n'est pas un carré modulo 257.

6. (**1 point**) On admet que E est d'ordre 256. À quels groupes $(\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}, +)$ $(E, +)$ peut-il être isomorphe ?

Solution :
Le groupe $(E, +)$ est d'ordre 256 donc, par le théorème de structure, il est isomorphe à $(\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}, +)$ avec $d_1 \mid (257 - 1)$, $d_1 \mid d_2$ et $d_1 d_2 = 256$.
Comme $257 - 1 = 256 = 2^8$, on peut avoir
- $d_1 = 1$ et $d_2 = 256$;
- $d_1 = 2$ et $d_2 = 128$;
- $d_1 = 4$ et $d_2 = 64$;
- $d_1 = 8$ et $d_2 = 32$;
- $d_1 = 16$ et $d_2 = 16$.

7. (**1 point**) Montrer que dans $(\mathbb{Z}/256\mathbb{Z}, +)$, il n'existe qu'un seul élément $h \neq 0$ tel que $[2]h = 0$. En déduire que $(E, +) \not\simeq (\mathbb{Z}/256\mathbb{Z}, +)$.

Solution :
Si $[2]h = 0 \bmod 256$, alors $2h = 256k$, $k \in \mathbb{Z}$ et $h = 128k$. Ainsi, modulo 256, $h = 0$ ou $h = 128$ et 128 le seul non nul.
Comme dans $\mathbb{Z}/256\mathbb{Z}$, il n'y a qu'un élément d'ordre 2 et que dans E, il y en a 3, on en déduit que $(E, +) \not\simeq (\mathbb{Z}/256\mathbb{Z}, +)$.

8. (**1,5 point**) On souhaite maintenant déterminer la structure de groupe exacte de E.
Soit $(G,+) = (\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}, +)$ avec d_1 qui divise d_2. Montrer que pour tout $h \in G$, l'ordre de h divise d_2 et montrer qu'il existe un élément g d'ordre d_2 dans G.

Solution :
Pour $h = (x, y)$, l'ordre de h est le plus petit entier positif n tel que $[n]h = (nx \bmod d_1, ny \bmod d_2) = (0, 0)$. Or, puisque d_1 divise d_2, on a $[d_2]h = (d_2x \bmod d_1, d_2y \bmod d_2) = (0, 0)$, d'où d_2 est un multiple de l'ordre de h.
Comme 1 est d'ordre d_2 dans $\mathbb{Z}/d_2\mathbb{Z}$, alors $(0, 1)$ est d'ordre d_2 dans G.

9. (**1,75 point**) On considère le point $P = (29, 17)$. On admet qu'il est dans E.
Calculer $[2]P$. On pourra utiliser les résultats suivants dans les calculs
   - $29^2 = 70 \bmod 257$;
   - $257 \times 9 - 34 \times 68 = 1$;
   - $3060 = 12 \times 257 - 24$.

Solution :
Notons $[2]P = (x, y)$. $\lambda = \frac{3x_P^2+2}{2y_P} = \frac{3\times 29^2+2}{34} = \frac{3\times 70+2}{34} = \frac{212}{34}$. D'après la relation de Bézout donnée, -68 est un inverse de 34 modulo 257 donc $\lambda = 212 \times (-68) = (-45) \times (-68) = 3060 = -24 \bmod 257$ donc
   - $x = \lambda^2 - x_P - x_P = (-24)^2 - 29 - 29 = 62 - 58 = 4 \bmod 257$;
   - $y = \lambda(x_P - x) - y_P = -24 \times (29 - 4) - 17 = 171 - 17 = 154 \bmod 257$.

$[2]P = (4, 154)$. Nous pouvons ainsi remarquer que E contient bien des points d'abscisse 4, le second étant naturellement $(4, 257 - 154) = (4, 103)$.

10. (**0,5 point**) On admet que $[8]P$ est le point d'abscisse nulle de la troisième question. Quel est l'ordre de P dans E ?

Solution :
Comme E est d'ordre $256 = 2^8$, P est d'ordre une puissance de 2. Comme $[2]P$ et $[8]P$ ne sont pas le neutre, on sait que P n'est pas d'ordre 1, 2 ou 8. Si P était d'ordre 4, on aurait alors $(0, 0) = [8]P = [2]([4]P) = [2]\mathcal{O} = \mathcal{O}$, d'où P est d'ordre au moins 16.
Or $[16]P = [2]([8]P) = [2](0, 0) = \mathcal{O}$ donc P est d'ordre 16.

11. (**1,5 point**) Soit $Q = (5, 69)$. Sachant que $[7]Q = (219, 214)$, montrer que $[8]Q = (68, 0)$. On pourra utiliser les résultats ou les indices suivants dans les calculs
   - $257 \times 5 - 214 \times 6 = 1$;
   - $158^2 = 35 \bmod 257$;
   - $158 \times (-63) = 69 \bmod 257$.

Solution :
Notons $[8]Q = (x, y)$. $\lambda = \frac{y_{[7]Q}-y_Q}{x_{[7]Q}-x_Q} = \frac{214-69}{219-5} = \frac{145}{214} = 145 \times (-6) = -870 = 158 \bmod 257$ donc
   - $x = \lambda^2 - x_Q - x_{[7]Q} = 158^2 - 5 - 219 = 35 - 5 - 219 = -189 = 68 \bmod 257$;
   - on peut s'arrêter ici car on sait déjà que le seul point d'abscisse 68 est $(68, 0)$.
     Au cas où, $y = \lambda(x_Q - x) - y_Q = 158 \times (5 - 68) - 69 = 158 \times (-63) - 69 = 69 - 69 = 0 \bmod 17$.

$[8]Q = (68, 0)$.

12. (**0,25 point**) Quel est l'ordre de Q ?

Solution :
Comme dans le cas de P, Q est d'ordre une puissance de 2 et $[8]Q = (68, 0)$, qui est d'ordre 2. Donc $[16]Q = \mathcal{O}$ et Q est d'ordre 16.

13. (**1,5 point**) On admet que l'ensemble des $[i]P + [j]Q$ sont tous distincts deux à deux pour $0 \leqslant i, j \leqslant 15$. Que peut-on en déduire sur le sous-groupe de E qu'ils engendrent ?
Montrer que ces points $[i]P+[j]Q$ sont tous d'ordre au plus 16. En déduire que $(E, +) \simeq (\mathbb{Z}/16\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}, +)$.

Solution :
On a $16 \times 16 = 256$ points de la sorte. Or E est d'ordre 256 donc il s'agit de tous les points de E.
On a $[16]([i]P + [j]Q) = [i]([16]P) + [j](16[Q]) = [i]\mathcal{O} + [j]\mathcal{O} = \mathcal{O}$ donc les points sont d'ordre au plus 16.
Ainsi $d_2 \leqslant 16$ et comme P et Q sont d'ordre 16, on en déduit que $d_1 = d_2 = 16$.

14. (**1 point**) Que peut-on déduire de la difficulté du DLP dans $(E, +)$ comparé à celui dans $(\mathbb{F}_{257}^*, \cdot)$?

Solution :
$\mathbb{F}_{257}^*$ est un groupe cyclique d'ordre 256. $(E, +)$ est un groupe d'ordre 256 mais chaque élément y est d'ordre au plus 16, ainsi en pratique le DLP s'effectuera dans un sous-groupe cyclique de taille 16. Or $16^2 = 256$, autrement dit la taille de 256 est deux fois celle de 16 et le DLP dans $(E, +)$ y est donc plus facile !

