Examen de Cryptologie
1re session

15 mai 2024
Durée 2h

Auteurs
Jérémy Berthomieu & Valérie Ménissier-Morain

Version du 15 mai 2024

Le seul document autorisé est une feuille manuscrite A4 recto-verso.
L'utilisation d'un appareil électronique est proscrite pendant toute la durée de l'épreuve.
Les exercices sont indépendants, il est donc interdit d'utiliser les hypothèses d'un exercice pour répondre aux questions d'un autre exercice.
Le barème sur 25 points est indicatif. La note finale sera le minimum entre les points obtenus et 20.

Exercice 1 – Cours – 6 points

1. **(2,5 points)** Qu'est-ce que le DLP ? Donner un algorithme pour le résoudre et sa complexité. Existe-t-il des groupes pour lesquels des algorithmes bien meilleurs existent ? Si oui, quels groupes et quels algorithmes ?

   Solution :
   Le DLP est le problème du logarithme discret, c'est-à-dire étant donné un groupe G, $g \in G$ et $h \in \langle g \rangle$, déterminer m tel que $g^m = h$. Le problème peut se résoudre via l'algorithme du *Baby step Giant step* dont la complexité est $O(\sqrt{n})$ où $n = |G|$.
   Le DLP se résout bien plus facilement dans les groupes $\mathbb{Z}/n\mathbb{Z}$ en utilisant l'algorithme d'Euclide étendu, la complexité est alors $O((\log n)^2)$.

2. **(3,5 points)** Donner les paramètres de RSA, en précisant leurs relations et lesquels sont publiques et privés. Donner une attaque par canaux auxiliaires sur RSA et un moyen de prévenir cette attaque.

   Solution :
   Les paramètres de RSA sont deux nombres premiers distincts p et q, leur produit $n = pq$. Il y a aussi un exposant de chiffrement e et son inverse, l'exposant de déchiffrement, d modulo $\varphi(n) = (p-1)(q-1)$.
   Les paramètres publiques sont en bleu et ceux privés en rouge.
   — 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 – Courbe elliptique – 8,5 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 $y^2 = x^3 + 3x$ 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 $\mathbb{F}_p$ avec $p = 17$ premier, $a = 3$ et $b = 0$. Elle semble donc elliptique.

Elle est elliptique si, et seulement si, $\Delta = -16(4a^3 + 27b^2) \neq 0$. Or $4a^3 + 27b^2 = 4 \times 3 + 27 \times 0^2 = 12 \neq 0$ et $\Delta \neq 0$.

2. **(Points de la courbe – 3,25 points)** Donner, sous la forme d'un tableau comme vu en cours/TD, l'ensemble des points rationnels définissant E.

Astuce : pour réduire la quantité de calculs, on pourra noter que $(-x)^3 + 3(-x) = -(x^3 + 3x)$.

Solution :

On calcule $x^3 + 3x$ mod 17 et y^2 mod 17 pour $x, y \in \mathbb{Z}/17\mathbb{Z}$. On regarde les collisions de ces deux listes et on déduit les points finis de la courbe.

y	y^2 mod 17
0	0
± 1	1
± 2	4
± 3	9
± 4	16
± 5	8
± 6	2
± 7	15
± 8	13

x	$x^3 + 3x$ mod 17	collision	(x, y)
0	0	✓ $y = 0$	$(0, 0)$
1	4	✓ $y = \pm 2$	$(1, \pm 2)$
2	14		
3	2	✓ $y = \pm 6$	$(3, \pm 6)$
4	8	✓ $y = \pm 5$	$(4, \pm 5)$
5	4	✓ $y = \pm 2$	$(5, \pm 2)$
6	13	✓ $y = \pm 8$	$(6, \pm 8)$
7	7		
8	9	✓ $y = \pm 3$	$(8, \pm 3)$
$9 = -8$	$-9 = 8$	✓ $y = \pm 5$	$(9, \pm 5)$
$10 = -7$	$-7 = 10$		
$11 = -6$	$-13 = 4$	✓ $y = \pm 2$	$(11, \pm 2)$
$12 = -5$	$-4 = 13$	✓ $y = \pm 8$	$(12, \pm 8)$
$13 = -4$	$-8 = 9$	✓ $y = \pm 3$	$(13, \pm 3)$
$14 = -3$	$-2 = 15$	✓ $y = \pm 7$	$(14, \pm 7)$
$15 = -2$	$-14 = 3$		
$16 = -1$	$-4 = 13$	✓ $y = \pm 8$	$(16, \pm 8)$

3. **(Points d'ordre 2 – 0,5 point)** Quels sont les points d'ordre 2 de la courbe E ?

Solution :
Un point d'ordre 2 a une ordonnée nulle. Il y a un seul point d'ordonnée nulle : $(0, 0)$.

4. (**Cardinal – 1 point**) Vérifiez que la courbe est de cardinal $n = 26$.

Solution :
Les points rationnels de la courbe sont
— 6 quadruplets symétriques de la forme $(x, \pm y), (-x, \pm 4y)$, à savoir $(1, \pm 2), (16, \pm 8), (3, \pm 6), (14, \pm 7), (4, \pm 5), (13, \pm 3), (5, \pm 2), (12, \pm 8), (6, \pm 8), (11, \pm 2), (8, \pm 3), (9, \pm 5)$
— 1 point sur l'axe des ordonnées $(0, 0)$
soit 25 points rationnels, auxquels il faut ajouter $\mathcal{O}$ le point à l'infini, ce qui fait donc 26 points au total.

5. (**Ordres possibles des éléments – 1 point**) Quels sont les ordres possibles des éléments de E ?

Solution :
E est de cardinal, donc d'ordre, 26. D'après le théorème de Lagrange, l'ordre des éléments d'un groupe divise l'ordre du groupe. Par conséquent les ordres possibles des éléments de E sont les diviseurs de 26 : 1, 2, 13 ou 26 .

6. (**Structure du groupe – 1,75 points**) Quelle est la structure de E ? Vous justifierez votre réponse.

Solution :
D'après le théorème de structure, E est isomorphe à $(\mathbb{Z}/d_1\mathbb{Z}, +) \times (\mathbb{Z}/d_2\mathbb{Z}, +)$ avec $d_1\, d_2 = n$, $d_1 \mid d_2$ et $d_1 \mid (p-1)$.
Deux raisonnements sont possibles :

1. De $d_1 d_2 = n$ et $d_1 \mid d_2$, on en déduit que d_1^2 divise n. Mais 26 n'admet pas de facteur carré autre que 1 donc $d_1 = 1$ et $d_2 = 26$.
2. — $p = 17$ donc d_1 doit être un diviseur de $17 - 1 = 16$, soit 1, 2, 4, 8 ou 16.
   — $n = 26$ n'est pas multiple de 4 donc les valeurs 4, 8 ou 16 de d_1 sont écartées.
   — Si $d_1 = 2$ alors d_2 est aussi multiple de 2 donc $d_1 d_2$ doit être multiple de $2 \times 2 = 4$. Or $n = d_1 d_2 = 26$ n'est pas multiple de 4 donc il nous faut aussi écarter la valeur 2 pour d_1.
   — Il ne reste que $d_1 = 1$, $d_2 = 26$.
   Autrement dit $E \simeq \mathbb{Z}/26\mathbb{Z}$.

Exercice 3 – Diffie-Hellman-Merkle – 10,5 points

On considère le groupe E de la courbe elliptique définie par l'équation $y^2 = x^3 + 3x$ sur $\mathbb{Z}/17\mathbb{Z}$ qui est d'ordre 26 et un générateur $G = (3, 6)$ de E.

Alice et Bob propose de faire un échange de clef via le protocole Diffie-Hellman-Merkle dans E avec le générateur G.

1. (**4 points**) La clef secrète d'Alice est $\alpha = 3$. Montrer qu'elle envoie $A = (5, 15)$ à Bob.

Solution :
Alice envoie $A = [3]G$ à Bob.
— On calcule tout d'abord $[2]G$:

$$\lambda = \frac{3x_G^2 + a}{2y_G} = \frac{3 \times 3^2 + 3}{2 \times 6} = \frac{30}{12} = \frac{5}{2} = 5 \times 9 = 45 = 11 \bmod 17$$

donc $[2]G = (x_{[2]G}, y_{[2]G})$ avec
$x_{[2]G} = \lambda^2 - 2x_G = 11^2 - 2 \times 3 = 36 - 6 = 30 = 13 \bmod 17$
et $y_{[2]G} = \lambda(x_G - x_{[2]G}) - y_G = 11 \times (3 - 13) - 6 = -6(-10) - 6 = 54 = 3 \bmod 17$.

— On calcule ensuite $A = [3]G = G + [2]G$:

$$\lambda = \frac{y_{[2]G} - y_G}{x_{[2]G} - x_G} = \frac{3 - 6}{13 - 3} = \frac{-3}{10} = 15 \bmod 17$$

donc $A = G + [2]G = (x_A, y_A)$ avec
$x_A = \lambda^2 - x_G - x_{[2]G} = 15^2 - 3 - 13 = 5 \bmod 17$
et $y_A = \lambda(x_G - x_A) - y_G = 15 \times (3 - 5) - 6 = 15 \bmod 17$.

Alice envoie donc le point $A = (5, 15)$.

2. (**2 points**) Alice reçoit $B = (3, 11)$ de la part de Bob. Afin d'être sûrs de leurs échanges, Alice et Bob se sont mis d'accord pour signer un point (x, y) de E en signant $x + 11y + 1$ avec du RSA. La clef publique RSA de Bob est $n = 187$ et $d = 3$.
La signature reçue est $s = 5$. Bob a-t-il envoyé la clef B ?

Solution :
Il suffit de calculer $s^d \bmod 187$ d'une part et $x + 11y + 1$ avec $(x, y) = (3, 11)$ d'autre part.
— $5^3 \bmod 187 = 125$.
— $3 + 11 \times 11 + 1 = 125$.
Les valeurs concordent donc Bob a bien signé ce point.

3. (**1,5 point**) Quelle est la clef secrète partagée par Alice et Bob ?

Solution :
La clef secrète partagée est $K = [\alpha]B = [3](3, 11)$.
Or $(3, 11)$ est l'opposé de $(3, 6)$ donc $[3](3, 11)$ est l'opposé de $[3](3, 6) = (5, 15)$ donc il s'agit de $(5, 2)$.

4. (**3 points**) Bob est tête-en-l'air, afin de ne pas oublier le point K, il l'écrit sur un post-it collé à son ordinateur. Ève voit le post-it plié et déchiré et ne peut y lire que $(.5, ..)$.
Quel calcul Ève peut-elle faire pour déterminer x_K ?

Solution :
On a deux possibilités pour x_K : 5 ou 15. Ève peut utiliser le symbole de Legendre pour déterminer si $x_K^3 + 3x_K$ est un carré ou non.
— Pour $x_K = 5$, on a $x_K^3 + 3x_K = 4 \bmod 17$, qui est clairement un carré.
— Pour $x_K = 15$, on a $x_K^3 + 3x_K = 3 \bmod 17$. Donc $(\frac{3}{17}) = (\frac{17}{3}) = (\frac{2}{3}) = -1$ donc 3 n'est pas un carré.
Ainsi, seul 5 peut être l'abscisse de K.