Examen de seconde session de Cryptologie
12 juin 2013

Auteurs
Guénaël Renault

Version du 21 avril 2017

Les seuls documents autorisés sont les slides du cours.
L'utilisation d'un appareil électronique est proscrit pendant toute la durée de l'épreuve.

Exercice 1 – Courbe elliptique (6 points)

Dans tout cet exercice, nous étudierons la courbe elliptique $\mathcal{E}$ définie sur le corps fini $\mathbb{F}_{11}$ par l'équation

$$\mathcal{E}: \quad y^2 = x^3 + 2x + 2$$

1. (**1.5 points**) Montrer que le groupe E construit à partir de $\mathcal{E}$ est de cardinal 9 et qu'il ne possède aucun élément d'ordre pair.

Solution :
On peut répondre facilement à cette question en construisant le tableau qui suit, la colonne des symboles de Legendre suffit.

x	$z = x^3 + 2x + 2 \mod 11$	$\left(\frac{z}{11}\right)$	$(x, y) \in E$
0	2	-1	
1	5	1	$(1,4), (1,7)$
2	3	1	$(2,5), (2,6)$
3	2	-1	
4	8	-1	
5	5	1	$(5,4), (5,7)$
6	10	-1	
7	7	-1	
8	2	-1	
9	1	1	$(9,1), (9,10)$
10	10	-1	

Sémantique du symbole de Legendre : $\left(\frac{z}{11}\right)$ vaut 1 si z est un carré modulo 11, -1 si z n'est pas un carré modulo 11 et 0 si 11 divise z.

Calcul du symbole de Legendre :
— 1 est le carré de 1 modulo tout nombre donc $\left(\frac{1}{p}\right) = 1$ pour tout p.
— $\left(\frac{2}{11}\right) = -1$ d'après la loi de réciprocité quadratique puisque $11 \equiv \pm 3 \mod 8$.
— $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right)$ d'après la loi de réciprocité quadratique car $3 \equiv 3 \mod 4$ et $11 \equiv 3 \mod 4$. $\left(\frac{11}{3}\right) = \left(\frac{2}{3}\right)$ car $11 \equiv 2 \mod 3$. Enfin $\left(\frac{2}{3}\right) = -1$ d'après la loi de réciprocité quadratique puisque $3 \equiv \pm 3 \mod 8$. Par conséquent $\left(\frac{3}{11}\right) = 1$.

— $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right)$ d'après la loi de réciprocité quadratique car $5 \equiv 1 \bmod 4$. $\left(\frac{11}{5}\right) = \left(\frac{1}{5}\right)$ puisque $11 \equiv 1 \bmod 5$ et $\left(\frac{1}{5}\right) = 1$ donc $\left(\frac{5}{11}\right) = 1$.

— $\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right)$ d'après la loi de réciprocité quadratique car $7 \equiv 3 \bmod 4$ et $11 \equiv 3 \bmod 4$. $\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right)$ car $11 \equiv 4 \bmod 7$. $\left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2$ et $\left(\frac{2}{7}\right) = -1$ d'après la loi de réciprocité quiadratique puisque $7 \equiv -1 \bmod 4$ donc $\left(\frac{4}{7}\right) = 1$ et $\left(\frac{7}{11}\right) = -1$.

— $\left(\frac{8}{11}\right) = \left(\frac{2}{11}\right)^3 = (-1)^3 = -1$.

— $\left(\frac{10}{11}\right) = \left(\frac{-1}{11}\right)$ puisque $10 \equiv -1 \bmod 11$. Or $\left(\frac{-1}{11}\right) = -1$ d'après la loi de réciprocité quadratique puisque $11 \equiv -1 \bmod 4$.

Nota : Sans passer par le symbole de Legendre on calcule la table de y^2 et on apparie les x et les y tels que $y^2 = z$.

Détermination des points : Lorsque $\left(\frac{z}{11}\right) = 1$, on lit dans la table des carrés (préalablement calculée) les différentes valeurs de y pour lesquels $y^2 = z$ et on en déduit les points (x, y) associés. Il y a donc 8 points rationnels, avec le point à l'infini cela fait donc 9 pour l'ordre du groupe E.

2. (**2 points**) Soit $P_1 = (2, 5)$ un élément de E. Calculer $[2]P_1$ et en déduire que P_1 est d'ordre 9. Donner la structure du groupe E (Argumenter votre réponse).

Solution :
$[2]P_1 = P_4$ de coordonnées (x_4, y_4) définies par :

$$\lambda = \frac{3x_2^2 + a}{2y_2} = \frac{3 * 2^2 + 2}{2 * 5} = 14 * 10^{-1} \mod 11 = 14 * 10 \mod 11 = 8 \mod 11,$$

d'où $x_4 = \lambda^2 - x_2 - x_2 = 8^2 - 2 - 2 = 60 \mod 11 = 5 \mod 11$, $y_4 = \lambda(x_2 - x_4) - y_2 = -8 * (2 - 5) - 5 = -29 = 4 \mod 11$. $P_4 = (5, 4)$.
Comme $P_4 = [2]P_1$ n'est pas l'opposé de P_1 (ils n'ont pas la même abscisse) et que les seuls ordres non triviaux sont 3 et 9, on ne peut avoir $[3]P_1 = P_4 + P_1 = \mathcal{O}$ et on en conclut que P_1 est bien d'ordre 9.

3. (**1.5 points**) Montrer, sans faire aucun calcul, que E ne contient que 2 points d'ordre 3 et montrer qu'ils sont opposés l'un de l'autre.

Solution :
Il y a un point d'ordre 9 donc E est isomorphe à $(\mathbb{Z}/9\mathbb{Z}, +)$ et dans $\mathbb{Z}/9\mathbb{Z}$ il n'y a que deux points d'ordre 3 : les diviseurs propres de 9, soit 3 et $6 = -3$.

4. (**1 point**) Exhiber les deux points d'ordre 3 de la question précédente.

Solution :
Il s'agit de $[3]P_1$ et $[6]P_1$. On calcule $[3]P_1 = P_1 + P_4$ et on en déduit son opposé $[6]P_1$.

Exercice 2 – RSA (5 points)

1. (**1 point**) Soit (n, e) une clé publique RSA. Pour $n = 21$, exhiber toutes les valeurs possibles pour e. Plus généralement, pour $n = pq$ donné, expliquer de manière concise comment choisir e judicieusement.

Solution :
$n = 3 * 7$ donc $\varphi(n) = 2 * 6 = 12$. e doit être un nombre compris entre 2 et 20 et inversible modulo φ donc premier avec 20, les valeurs possibles sont 5, 7 et 11. Il faut que $ed = 1 \bmod \varphi(n)$ et que la racine e-ième soit difficile à calculer.

2. (**2 points**) Soit $n = 221$ un module RSA et $d = 121$ un exposant de déchiffrement. Déchiffrer le chiffré $C = 2$ en utilisant le CRT. Que pensez-vous d'un tel message ?

Solution :
On calcule tout d'abord la factorisation de $n = 221 = 225 - 4 = 15^2 - 2^2 = (15 - 2) * (15 + 2) = 13 * 17$.
On doit calculer $C^d \bmod n$, pour cela on va calculer $C^d \bmod 13 = C^{d \bmod 13} \bmod 13$ et $C^d \bmod 17 = C^{d \bmod 17} \bmod 17$:
- $d \bmod 12 = 1$ donc $C^{d \bmod 12} \bmod 13 = 2^1 \bmod 13 = 2 \bmod 13$.
- $d \bmod 16 = 9$ donc $C^{d \bmod 16} \bmod 17 = 2^9 \bmod 17 = (2^4)^2 * 2 = (-1)^2 * 2 = 2 \bmod 17$.

On sait donc que
$$C^d = \begin{cases} 2 \bmod 13 \\ 2 \bmod 17 \end{cases}$$
on en déduit donc que le clair $C^d = 2 \bmod 13 * 17 = 2 \bmod n$. Le clair et le chiffré sont identiques, le choix du couple (e, d) n'est pas très convaincant et le message n'est pas bien protégé.

3. (**2 points**) Un attaquant collecte l'ensemble des clés publiques de S serveurs web accessibles librement. On suppose ici que tous les modules RSA ainsi collectés sont de la même taille t. Estimer, en fonction de t et S, la complexité de trouver, s'il existe, un couple de modules qui puissent se factoriser facilement. Donner une borne sur S pour que ce calcul reste polynomial en t. (Vous donnerez et expliquerez l'algorithme dont vous estimerez la complexité.)

Solution :

Exercice 3 – Vigenère (6 points)

On suppose dans tout cet exercice que les clés utilisées dans les chiffrements sont toutes composées de caractères distincts deux à deux.

1. (**3 points**) Soit E_{K_1} et E_{K_2} deux chiffrements de Vigenère de clés respectives K_1 et K_2. Soit le chiffrement E_K qui consiste à chiffrer un message M en C de la manière suivante
$$C = E_K(M) = E_{K_2}(E_{K_1}(M))\,.$$
Montrer que E_K est un chiffrement de Vigenère dont vous donnerez la clé K et sa longueur.

Solution :
$\ell(K) = \text{ppcm}(\ell(K_1), \ell(K_2))$ et $K = E\ \underbrace{K_2 \ldots K_2}_{\ell(K)/\ell(K_2)\text{fois}}\ (\ \underbrace{K_1 \ldots K_1}_{\ell(K)/\ell(K_1)\text{fois}}\ )$.

2. (**1 point**) Chiffrer le message `ATTAQUEMAINTENANT` avec le procédé de la question précédente et les clés $K_1 =$ `ABC` et $K_2 =$ `XY`.

Solution :
On chiffre d'abord avec K_1 ce qui donne

```
  ATTAQUEMAINTENANT
+ ABCABCABCABCABCAB
-------------------
  AUVARWENCIOVEOCNU
```

puis celui avec K_2 ce qui donne

```
  AUVARWENCIOVEOCNU
+ XYXYXYXYXYXYXYXYX
-------------------
  XSSYOUBLZGLTBMZLR
```

3. (**2 points**) Soit un texte de longueur ℓ produit de deux nombres premiers distincts. En supposant que l'alphabet soit aussi grand qu'on le souhaite, montrer que l'on peut construire deux clés K_1 et K_2 tel que le procédé de la question 1 soit un chiffrement parfait.

Solution :
Si $\ell = pq$ alors on prend une clef K_1 de longueur p et une clef K_2 de longueur K_2, on construit ainsi un chiffrement de Vigenère de longueur de clef pq c'est-à-dire la longueur du message à chiffrer donc on obtient un chiffrement parfait.

Exercice 4 – Questions de cours et de bon sens cryptologique (4 points)

1. (**1 point**) Quels sont les algorithmes que vous conseillerez pour faire du chiffrement de données ? Pour faire de l'authentification numérique ?

Solution :
Données : chiffrement symétrique après échange de clefs par RSA. Authentification : RSA.

2. (**1 point**) Rappeler quel est l'unique chiffrement parfait. Pourquoi le chiffrement parfait n'est pas utilisé en pratique, par exemple pour le paiement sur internet ?

Solution :
Celui de Vernam (One Time Pad). Il n'est pas possible de convenir à l'avance d'une clef aussi longue que le message à faire parvenir entre le commerçant et le client d'autant que la clef ne peut servir qu'une seule fois.

3. (**1 points**) Pourquoi est-il dangereux d'avoir un mot de passe court (de taille 4 par exemple) et utilisant les 26 caractères de l'alphabet ? (Vous décrirez un scénario d'attaque.)

Solution :
$26^4 < 500000$ ce n'est rien à explorer par force brute.

4. (**1 point**) Pourquoi les générateurs pseudo-aléatoires sont-ils sensibles en cryptologie ?

Solution :