Examen de Cryptologie
1re session
10 mai 2022
Durée 2h

Version du 10 mai 2022

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.
Le barème sur 40 points est indicatif. La note finale sera le minimum entre les points obtenus et 20.

Exercice 1 – Théorème des restes chinois – 8 points

1. (**Algorithme d'Euclide étendu – 2 points**) En utilisant l'algorithme d'Euclide étendu, montrer que 7 est inversible mod 165 et calculer son inverse.
2. (**2 points**) Soit $N = 2^{100}$. Montrer que
$$\begin{cases} N = 1 \bmod 3 \\ N = 1 \bmod 5 \\ N = 2 \bmod 7 \\ N = 1 \bmod 11 \end{cases}$$
3. (**1 point**) En déduire que $N = 1 \bmod 165$.
4. (**3 points**) Quel est le reste de la division euclidienne de 2^{100} par 1155 ?

Exercice 2 – Courbe elliptique – 14,5 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 $y^2 = x^3 + x + 3$ sur $\mathbb{F}_{11}$.

1. (**1 point**) Justifier que cette courbe est bien elliptique.
2. (**Points de la courbe – 3 points**) Donner, sous la forme d'un tableau comme vu en cours/TD, l'ensemble des points rationnels définissant E.
3. (**Points d'ordre 2 – 0,5 point**) Quels sont les points d'ordre 2 de la courbe E ?
4. (**Cardinal – 1 point**) Vérifiez que la courbe est de cardinal $n = 18$.
5. (**Ordres possibles des éléments – 1 point**) Quels sont les ordres possibles des éléments de E.
6. (**Calcul dans E – 3 points**) Soient $P_1 = (5, 1)$ et $P_2 = (0, 6)$ deux points de E. Montrez que $[3]P_1 = P_2$.
7. (**Structure du groupe – 3 points**) Quelle est la structure de E ? Vous justifierez votre réponse.
8. (**Maximalité de la courbe – 2 points**) Montrez qu'il n'existe pas de courbe elliptique de cardinal supérieur à 18 sur $\mathbb{F}_{11}$.

Exercice 3 – Logarithme discret – 18 points

1. (**$\mathbb{F}_{47}^{\times}$ – 2 points**) Rappelez ce qu'est $\mathbb{F}_{47}^{\times}$. Quels sont ces éléments ? Quel est son cardinal ? Montrez que 16 est d'ordre 23 dans le groupe multiplicatif $\mathbb{F}_{47}^{\times}$.

On va s'intéresser à la résolution de deux façons du DLP dans le sous-groupe de $\mathbb{F}_{47}^{\times}$ engendré par 16.

2. (**Baby-Step-Giant-Step – 5 points**)

   (a) (**Baby-Step-Giant-Step – 3 points**) En utilisant l'algorithme Baby-Step-Giant-Step, calculez le logarithme discret de 17 en base 16, c'est-à-dire le plus petit entier k tel que $16^k = 17 \bmod 47$.

   (b) (**Exponentiation – 2 points**) Vous vérifierez le résultat de la question précédente en reprenant l'algorithme d'exponentiation Square-and-Multiply, dont vous donnerez la complexité.

3. (**Méthode ρ de Pollard – 11 points**)
   On s'intéresse à présent à un autre algorithme permettant également de résoudre le problème du logarithme discret. Pour cela, on se place dans un sous-groupe $\langle h \rangle$ d'ordre q de $G = (\mathbb{Z}/p\mathbb{Z})^{\times}$, où p et q sont premiers.
   Soit n un élément de $\langle h \rangle$, on définit l'application $f : \langle h \rangle \times \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to \langle h \rangle \times \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ par :

$$f((x,a,b)) = \begin{cases} (hx, a+1, b) & \text{si } x = 0 \bmod 3 \\ (nx, a, b+1) & \text{si } x = 1 \bmod 3 \\ (x^2, 2a, 2b) & \text{si } x = 2 \bmod 3 \end{cases}$$

   On construit la suite

$$\begin{cases} (x_0, a_0, b_0) = (1, 0, 0) \\ (x_{i+1}, a_{i+1}, b_{i+1}) = f((x_i, a_i, b_i)) \end{cases}$$

   (a) (**Cycle – 1 point**) Sans effectuer de calcul expliquez pourquoi la suite $(x_i)_{i\in\mathbb{N}}$ possède un cycle.

   (b) (**Relation dans le triplet – 2 points**) Montrez que pour tout i, $x_i = h^{a_i} n^{b_i}$.

   (c) (**Principe de résolution du DLP – 1,5 point**) Montrez que $c = (a_i - a_j)(b_j - b_i)^{-1} \bmod q$ donne le logarithme discret de n en base h, lorsque $x_j = x_i$, et $b_j - b_i$ est inversible modulo q.

   (d) (**Cycle à exploiter – 1,5 point**) Justifiez qu'il existe un entier i tel que $x_i = x_{2i}$.

   (e) (**Application – 3 points**) Mettez alors en application cet algorithme pour retrouver le logarithme discret de 17 en base 16.

   (f) (**Complexité – 2 points**) On suppose que la fonction f est suffisamment aléatoire pour trouver un cycle en $\mathcal{O}(\sqrt{q})$ itérations. Quelle est alors la complexité en temps de cet algorithme.
   On calcule en parallèle les deux suites $(x_i)_{i\in\mathbb{N}}$ et $(x_{2i})_{i\in\mathbb{N}}$, jusqu'à trouver une collision. Combien d'éléments de $\langle h \rangle$ devez-vous stocker alors.
   Comparez les complexités en temps et en espace de cet algorithme avec celles de l'algorithme Baby-Step-Giant-Step.