Examen de Cryptologie

18 juin mai 2021

Durée 1h30

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.
2. (**RSA – 2 points**) a. Donner les relations qui lient les différents paramètres utilisés dans RSA.
   b. Parmi ces paramètres, lesquels sont publics et lesquels restent secrets ?

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.

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.
2. (**1 point**) Donner l'ensemble des carrés dans $\mathbb{F}_{17}$.
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.
4. (**1 point**) À l'aide du théorème de structure, montrer que soit $(E, +) \simeq (\mathbb{Z}/20\mathbb{Z}, +)$, soit $(E, +) \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}, +)$.
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 $(E, +) \not\simeq (\mathbb{Z}/20\mathbb{Z}, +)$.
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.
7. (**3 points**) Calculer $[5]Q$.
8. (**0,5 point**) En déduire que Q est d'ordre 10.
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.
10. (**0,5 point**) En déduire que $F = E$.

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.