SCIENCES SORBONNE UNIVERSITÉ

Examen de Cryptologie
1re session
14 mai 2025
Durée 2h

Version du 27 mai 2025

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 36 points est indicatif. La note finale sera le minimum entre les points obtenus et 20.

Exercice 1 – Cours – 9,5 points

1. (**RSA – 1,5 point**) Un utilisateur publie sa clef publique RSA (n, e). Pourquoi ne faut-il à aucun prix que $\varphi(n)$ ne fuite ?
2. (**Authentification – 2,5 points**) Sans entrer dans aucun détail algorithmique, expliquer le fonctionnement de l'authentification
   (a) en cryptographie à clef publique
   (b) en cryptographie à clef privée
3. (**Solutions d'une équation – 5,5 points**) En vous appuyant sur un algorithme vu en cours, expliquez comment vous pouvez vérifier qu'il existe des entiers x et y tels que $867 \times x + 666 \times y = 12$. Utilisez cet algorithme pour déterminer la forme de tous les couples d'entiers x et y qui vérifient cette équation. Vous justifierez vos calculs en détail.

Exercice 2 – Courbes elliptiques – 7 points

1. (**5 points**) Existe-t-il un groupe additif E de cardinal 12 défini à partir des points rationnels d'une courbe elliptique sur $\mathbb{F}_5$? Si oui, donnez l'équation qui définit cette courbe elliptique ; si non, expliquez pourquoi.
   Même question pour le cardinal 6 sur $\mathbb{F}_5$.
2. (**2 points**) L'ensemble des points rationnels d'équation $y^2 = x^3 - 2x + 1$ définit-il une courbe elliptique sur $\mathbb{F}_5$? Justifiez-le.
   Même question sur $\mathbb{F}_7$?

Exercice 3 – 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 $y^2 = x^3 + 2x - 2$ sur $\mathbb{F}_{11}$.

1. (**0,5 point**) Justifiez qu'il s'agit bien d'une courbe elliptique.
2. (**3 points**) Donner, sous la forme de tableaux comme vus en cours/TD, l'ensemble des points rationnels définissant E. Montrer que E est de cardinal 15.

3. (**4 points**) Expliquer pourquoi E est un groupe cyclique.
4. (**0,5 point**) Soit $P = (0, 3)$ et $Q = (1, 1)$; vérifier que ce sont bien deux points de E.
5. (**Calcul dans E – 3 points**) Calculer $[2]P$ et $P + Q$.
6. (**1,5 point**) Sachant que $Q = [4]P$, montrer que P n'est ni d'ordre 3 ni d'ordre 5.
7. (**2 points**) Exhiber un générateur de ce groupe. Justifiez votre réponse.

Exercice 4 – Carré ? – 5 points

317 est-il un carré modulo 521 ?