Examen de Cryptologie
1re session

15 mai 2024
Durée 2h

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 ?
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.

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.
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 $(-x)^3 + 3(-x) = -(x^3 + 3x)$.
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 $n = 26$.
5. **(Ordres possibles des éléments – 1 point)** Quels sont les ordres possibles des éléments de E ?
6. **(Structure du groupe – 1,75 points)** Quelle est la structure de E ? Vous justifierez votre réponse.

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