Examen de Cryptologie

14 mai 2019
Durée 2h

Version du 23 mai 2019

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* 34.

Exercice 1 – Questions – 2,5 points

1. (**0,5 point**) Qu'est-ce que le *social engineering* ? Donner deux exemples.
2. (**0,5 point**) Sur quelle faiblesse repose l'attaque de Wiener ?
3. (**1 point**) Que vous évoque le nom de Kocher ?
4. (**0,5 point**) Comment se nomme le protocole prédécesseur de TLS (*Transport Layer Security*) ? Donner le nom d'un logiciel ou d'une bibliothèque l'implémentant.

Exercice 2 – RSA – 11 points

1. (**Alice ouvre ses oreilles – 2.5 points**) Alice choisit $p = 17, q = 19$ et $e = 91$ pour chiffrer ses messages avec RSA. Quelle clef publique publie-t-elle et quelle clef privée conserve-t-elle par devers elle ? Vous détaillerez les calculs d'Alice.
2. (**Bob parle à Alice – 4.5 points**) Bob adresse à Alice les messages chiffrés $c_1 = 10$, $c_2 = 7$ et $c_3 = 16$. Alice déchiffre ces messages, quels messages clairs m_1, m_2 et m_3 obtient-elle ? Quels calculs effectuent-elles pour cela ? Que pensez-vous du message m_3 ?
3. (**RSA+CRT – 4 points**) Expliquer comment utiliser le CRT pour déchiffrer plus efficacement un message chiffré avec RSA et quel est le facteur gagné dans le cas d'une multiplication naïve et dans le cas d'une multiplication avec l'algorithme de Karatsuba.

Exercice 3 – DLP – 6,5 points

1. (**1 point**) On considère le groupe $G = \mathbb{F}_{53}^{\times}$. Quel est son ordre ? Est-il cyclique ?
2. (**0,5 point**) On considère $g = 2$ et $h = 37$. On souhaite calculer le plus petit entier a tel que $[a]g = g^a = h$ avec l'algorithme Baby-Step Giant-Step.
   Justifier que les pas de géant qu'il faut faire sont de taille $s = 8$.
3. (**1,5 point**) Calculer $[s]g = g^s$ puis son inverse dans G.
4. (**3,5 points**) Déterminer a à l'aide de l'algorithme Baby-Step Giant-Step.

Exercice 4 – Courbes Elliptiques – 14 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 $y^2 = x^3 + 2x + 1$ sur $\mathbb{F}_{13}$.

1. (**1 point**) Justifier que cette courbe est bien elliptique.
2. (**0.5 point**) Donner l'ensemble des carrés dans $\mathbb{F}_{13}$.
3. (**2 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 8.
4. (**0,5 point**) Soit $P = (8, 3)$ et $Q = (0, 12)$; vérifier que ce sont bien deux points de E.
5. (**1,5 point**) Montrer que $P + Q$ est un point d'ordre 2.
6. (**2 points**) Montrer que $Q = [3]P$.
7. (**0,5 point**) En déduire que P n'est ni d'ordre 2 ni d'ordre 4.
8. (**1 point**) Montrer que E est un groupe cyclique. Exhiber un générateur de ce groupe.
9. (**1 point**) Alice et Bob décident de procéder à un échange de clef *via* le protocole Diffie–Hellman–Merkle dans le groupe $(E, +)$.
   1. Ils se mettent d'accord pour prendre P comme générateur.
   2. Alice choisit comme clef secrète $a = 3$ et envoie $A = [a]P$ à Bob.
   3. Bob choisit comme clef secrète $b = 5$ et envoie $B = [b]P$ à Alice.

   Quelle est la clef privée partagée ?
10. (**0,5 point**) Justifier que le polynôme $t^2 - 2$ est irréductible dans $\mathbb{F}_{13}[t]$. En déduire que $\mathbb{F}_{169} = \mathbb{F}_{13}[t]/(t^2 - 2)$.
11. (**1 point**) On note E' le groupe additif défini à partir des points rationnels de la courbe elliptique définie par l'équation $y^2 = x^3 + 2x + 1$ sur $\mathbb{F}_{169}$. On admet que E' est d'ordre 160.
    En utilisant le théorème de structure, montrer que seules les situations suivantes sont possibles :

$$(E', +) \simeq (\mathbb{Z}/160\mathbb{Z}, +),$$
$$(E', +) \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/80\mathbb{Z}, +),$$
$$(E', +) \simeq (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}, +).$$

12. (**1,5 point**) Montrer que $x^3 + 2x + 1$ admet 2, $2t + 12$ et $11t + 12$ comme racines dans $\mathbb{F}_{169}$. Que peut-on en déduire sur le nombre de points d'ordre 2 dans E' ?
13. (**1 point**) Montrer que dans $(\mathbb{Z}/160\mathbb{Z}, +)$, il n'existe qu'un seul élément $h \neq 0$ tel que $[2]h = 0$. En déduire que $(E', +) \neq (\mathbb{Z}/160\mathbb{Z}, +)$.