Examen de Cryptologie

11 mai 2021
Durée 1h30

Version du 30 mai 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* 30*.*

Exercice 1 – Questions – 4 points

1. (**1 point**) On note $p > 2$ un nombre premier.
   Parmi les réponses suivantes, dire lequelles sont correctes en justifiant.
   La réciprocité quadratique permet de
   (a) savoir si -1 est un carré modulo p.
   (b) déterminer une racine carrée de 2 modulo p.
   (c) savoir que $q > 2$, un nombre premier, est un carré modulo p si, et seulement si, p est un carré modulo q.
   (d) savoir si $q > 2$, un nombre premier, est un carré modulo p suivant si p est un carré modulo q.
2. (**1 point**) Soient a et b deux entiers non nuls. Montrer que $\frac{a}{b} = [q_1, q_2, \ldots, q_r] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \frac{1}{q_r}}}$ où $q_1, q_2, \ldots, q_r$ sont les quotients apparaissant dans l'algorithme d'Euclide appelé avec a et b.
3. (**1 point**) Montrer que le DLP se résout en temps polynomial dans $(\mathbb{Z}/n\mathbb{Z}, +)$.
4. (**1 point**) Donner une attaque par canaux auxiliaires sur RSA et un moyen de prévenir cette attaque.

Exercice 2 – RSA – 8 points

Les 2 parties de l'exercice sont indépendantes.

Alice et Bob souhaitent communiquer en utilisant RSA. Alice crée donc une paire de clefs dont la clef publique est (n, e).

On s'intéresse à 2 scénarios.

1. (**Alice est naïve – 2,5 point**) Oscar a intercepté un chiffré $c = m^e \bmod n$. Dans un jour de gentillesse, Alice accepte de déchiffrer un message c' qu'Oscar choisirait si, seulement si, $c' \neq c$.
   Oscar calcule $c' = 2^e c \bmod n$.
   (a) (1 point) Si $c' = c$, montrer comment Oscar peut retrouver m.
   (b) (1,5 point) Si $c' \neq c$, montrer comment Oscar peut retrouver m.
2. (**Alice est amnésique – 5,5 points**) *Pour chacune des deux sous-questions, un raisonnement général est demandé avant d'effectuer les calculs correspondants.*
   La clef publique d'Alice est $(n, e) = (20099, 11857)$.

(a) (2 points) Alice a oublié quels premiers p et q elle a utilisés pour obtenir n. Mais sa clef privée contient $\varphi(n) = 19800$. Retrouver p et q, sans recherche exhaustive, avec l'hypothèse que $p < q$.
On pourra utiliser le fait que $98^2 = 9604$.

(b) (3,5 points) Vérifier que le choix de e est correct et déterminer le reste de la clef privée.

Exercice 3 – Courbes Elliptiques – 18 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 $y^2 = x^3 + 2x$ sur $\mathbb{F}_{257}$.

En utilisant aussi bien le représentant canonique $c \bmod n$ *que* $n - c$ *pour réduire la taille des nombres manipulés, seuls des calculs donnant lieu à des nombres à* 3 *chiffres maximum sont à effectuer, hormis à la question 9 où une opération a un résultat à* 4 *chiffres, De plus, pour les calculs les plus complexes des indications sont fournies.*

1. (**1 point**) Vérifier que 257 est bien premier.
2. (**1 point**) Justifier que cette courbe est bien elliptique.
3. (**2 points**) Déterminer, s'ils existent, les points d'abscisse 0 de E.
   Calculer 68^2 dans $\mathbb{F}_{257}$. En déduire que E admet au moins trois points d'ordonnée 0 dont $(68, 0)$.
4. (**2 points**) Montrer que E admet deux points d'abscisse 4 si, et seulement si, 72 est un carré modulo 257. Puis déterminer si E possède de tels points.
5. (**2 points**) Donner une condition nécessaire et suffisante pour que E admette deux points d'abscisse 8. Puis déterminer si E possède de tels points.
6. (**1 point**) On admet que E est d'ordre 256. À quels groupes $(\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}, +)$ $(E, +)$ peut-il être isomorphe ?
7. (**1 point**) Montrer que dans $(\mathbb{Z}/256\mathbb{Z}, +)$, il n'existe qu'un seul élément $h \neq 0$ tel que $[2]h = 0$. En déduire que $(E, +) \not\simeq (\mathbb{Z}/256\mathbb{Z}, +)$.
8. (**1,5 point**) On souhaite maintenant déterminer la structure de groupe exacte de E.
   Soit $(G, +) = (\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}, +)$ avec d_1 qui divise d_2. Montrer que pour tout $h \in G$, l'ordre de h divise d_2 et montrer qu'il existe un élément g d'ordre d_2 dans G.
9. (**1,75 point**) On considère le point $P = (29, 17)$. On admet qu'il est dans E.
   Calculer $[2]P$. On pourra utiliser les résultats suivants dans les calculs
   - $29^2 = 70 \bmod 257$;
   - $257 \times 9 - 34 \times 68 = 1$;
   - $3060 = 12 \times 257 - 24$.
10. (**0,5 point**) On admet que $[8]P$ est le point d'abscisse nulle de la troisième question. Quel est l'ordre de P dans E ?
11. (**1,5 point**) Soit $Q = (5, 69)$. Sachant que $[7]Q = (219, 214)$, montrer que $[8]Q = (68, 0)$. On pourra utiliser les résultats ou les indices suivants dans les calculs
    - $257 \times 5 - 214 \times 6 = 1$;
    - $158^2 = 35 \bmod 257$;
    - $158 \times (-63) = 69 \bmod 257$.
12. (**0,25 point**) Quel est l'ordre de Q ?
13. (**1,5 point**) On admet que l'ensemble des $[i]P + [j]Q$ sont tous distincts deux à deux pour $0 \leqslant i, j \leqslant 15$. Que peut-on en déduire sur le sous-groupe de E qu'ils engendrent ?
    Montrer que ces points $[i]P+[j]Q$ sont tous d'ordre au plus 16. En déduire que $(E, +) \simeq (\mathbb{Z}/16\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}, +)$.
14. (**1 point**) Que peut-on déduire de la difficulté du DLP dans $(E, +)$ comparé à celui dans $(\mathbb{F}^*_{257}, \cdot)$?

