Partiel de Cryptologie

16 mars 2022
Durée 1h30

Version du 22 avril 2022

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

Exercice 1 – Questions diverses – 5,5 points + 1 point bonus

1. (**1 point principe – 1 point bonus schéma**) Quel principe de sécurité est violé par le concept *Man In The Middle* ? Vous en expliquerez le mécanisme sur un exemple.
2. (**0.5 point**) Pourquoi ne peut-on pas utiliser la technique des indices de coïncidence et indices de coïncidence mutuelle pour déterminer la clé de chiffrement ou le texte clair correspondant à un texte chiffré par substitution ?
3. (**1 point**) Expliquez pourquoi la méthode de corrélation de Pearson donne de meilleurs résultats que la méthode des indices de coïncidence pour la cryptanalyse de Vigenère.
4. (**Algorithme d'Euclide étendu – 3 points**) En utilisant l'algorithme d'Euclide étendu, dites si $a = 819$ est inversible modulo $n = 861$? Si oui quel est son inverse ? Est-ce un diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$? Si oui exhibez un témoin de diviseur de zéro de a pour n.

   Mêmes questions pour $n = 859$.

   Vous justifierez rigoureusement vos réponses.

Exercice 2 – Message chiffré – 3 points pour le raisonnement + 2 points pour le message déchiffré

En 1627 commence le siège de La Rochelle, cité huguenote, par le roi de France. L'armée du Roi assiège la ville en bloquant tout d'abord tout ravitallement par voie de terre puis par la construction d'une digue en contrôlant l'accès du port.

Le maire de La Rochelle appelle leur allié anglais à la rescousse par le message suivant chiffré par la méthode de Vigenère

```
PMYMM UMRYV RQJYJ UITWI QWAMI QKKLG OMJYX RCZYT DZZHS XABIY
VLKGE QLUHW DAYCW WITWI SWALV RUVLI FMHFS FCYME QAJYP DQMIH
HNXIC PIOLI GMRUV RKNYP OM
```

Saurez-vous dire quel est le contenu de ce message ?
Vous détaillerez votre raisonnement.

Exercice 3 – Groupe fini – 12 points + 1,5 point de bonus

On considère l'ensemble $\mathcal{E}$ muni de la loi $\circ$, supposée associative. Les éléments de $\mathcal{E}$ sont tous de la forme $P = (x, y)$ avec x et y modulo 13 sauf un, noté $\mathcal{O}$. De plus, $P = (x, y) \in \mathcal{E}$ si, et seulement si, $y^2 = x^3 + 3x + 5 \mod 13$.

1. **(1 point)** Vérifier que $(1, 3), (4, 4), (12, 12) \in \mathcal{E}$.

On admet dans la suite qu'avec $(1, 10), (4, 9), (11, 2), (11, 11), (12, 1)$, ce sont les seuls éléments de $\mathcal{E} - \{\mathcal{O}\}$.

2. **(0,5 point)** Pour $P, Q \in \mathcal{E}$, on note $R = P \circ Q \in \mathcal{E}$. De plus,
   (i). si $Q = \mathcal{O}$, alors $R = P$, sinon si $P = \mathcal{O}$, alors $R = Q$;
   (ii). sinon, si $P = (x_1, y_1)$ et $Q = (x_1, -y_1)$, alors $R = \mathcal{O}$;
   (iii). sinon, $P = (x_1, y_1)$, $Q = (x_2, y_2) \neq (x_1, -y_1)$ et $R = (x_3, y_3)$ avec

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$$

   et $\lambda = 8(x_1^2 + 1)y_1^{-1} \mod 13$ si $P = Q$ ou $\lambda = (y_2 - y_1)(x_2 - x_1)^{-1} \mod 13$ sinon.

   Quel est le neutre pour $\circ$? Quel est l'inverse de $P \in \mathcal{E}$ pour $\circ$?
3. **(1 point)** Montrer que $(\mathcal{E}, \circ)$ est un groupe.
4. **(2 points+1 point bonus)** Justifier, de deux manières distinctes, s'il existe ou non des éléments d'ordre 2 dans $\mathcal{E}$.
5. **(3,5 points)** Montrer que $\circ$ est commutative.
6. **(1,5 point +0,5 point de bonus si (ii) dûment invoqué pour conclure)** Soient $P_0 = (4, 4)$ et $P_1 = (4, 9)$ dans $\mathcal{E}$. Montrer que $[3]P_i = P_i \circ P_i \circ P_i = \mathcal{O}$ pour $i \in \{0, 1\}$.
7. **(1,5 point)** Soit $Q = (12, 12)$. Montrer que $[3]Q = P_1$.
8. **(1 point)** $(\mathcal{E}, \circ)$ est-il cyclique ?

Exercice 4 – Divisibilité et PGCD – 7 points

Soient $a, b \in \mathbb{N}$ tels que $0 < a < b$.

1. **(1,5 point)** Montrer que si a divise b alors, pour tout $n \in \mathbb{N}$, $n^a - 1$ divise $n^b - 1$.
2. **(1,5 point)** Soit $n \in \mathbb{N}^*$, montrer que le reste de la division euclidienne de $n^b - 1$ par $n^a - 1$ est $n^r - 1$, où r est le reste de la division euclidienne de b par a.
3. **(1,5 point)** Soit $n \in \mathbb{N}^*$, montrer que $\text{pgcd}(n^b - 1, n^a - 1) = n^d - 1$, où $d := \text{pgcd}(a, b)$.
4. On rappelle que l'entier b vérifie $b > 1$.
   (a) **(0,5 point)** Soit $n \in \mathbb{N}$ tel que $n > 2$. Montrer que $n^b - 1$ est toujours composé.
   (b) **(1 point)** Montrer que si b est composé alors, $2^b - 1$ est composé.
   (c) **(1 point)** Donner une condition nécessaire pour que $n^b - 1$ soit premier.

   Les nombres premiers de cette forme sont appelés premiers de Mersenne. Ils sont très utiles car l'arithmétique modulo un premier de Mersenne est très efficace sur un ordinateur binaire. En cryptographie, ils sont notamment utilisés pour générer des nombres aléatoires.