# Partiel de Cryptologie

## 13 mars 2019
## Durée 1h45

Version du 26 mars 2019

*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 25 points (dont 3,5 de bonus) est indicatif.*

### Exercice 1 – Questions de base – 9,5 points

1. (**1 point**) Qu'est-ce que le surchiffrement ? Donnez un exemple célèbre.
2. (**3 points**) Quelles sont les solutions dans $\mathbb{Z}$ des équations : $4x + 2 = 5 \bmod 21$ ? $7x + 9 = 2 \bmod 21$ ? $3x + 1 = 2 \bmod 21$ ?
3. (**3 points**) 3743 est-il inversible dans $\mathbb{Z}/4541\mathbb{Z}$ ? si oui calculez son inverse ? Sinon, calculez un témoin de diviseur de 0 de 3743 dans $\mathbb{Z}/4541\mathbb{Z}$ ? Vous justifierez en détail les calculs effectués.
4. (**1,5 point**) Donner l'ensemble des entiers $n \in \{2, 3, 4, 5, 6\}$ tels que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Justifier. Donner l'ensemble des entiers $n \in \{2, 3, 4, 5, 6\}$ tels qu'il existe un corps à $n$ éléments. Justifier.
5. (**1 point**) Soit $G$ un groupe cyclique. Quel genre de problème dans $G$ l'algorithme du pas de bébé, pas de géant (*Baby-Step, Giant-Step*) est-il capable de résoudre ? Avec quelle complexité ?

### Exercice 2 – Déchiffrement d'un message par Vigenère – 2 points

Déchiffrer le message « `FUBHT FDNCP CFAE` » chiffré par le chiffrement de Vigenère avec la clé `PAX`.

### Exercice 3 – Cryptanalyse d'un chiffrement par transposition – 5 points

On rappelle ici le fonctionnement du chiffrement par transposition. On écrit le texte de gauche à droite sur $n$ colonnes. Si nécessaire on complète avec des "`X`" (*padding*). On applique une permutation sur ces colonnes. Enfin on lit colonne par colonne, de haut en bas, pour obtenir le texte chiffré.

Voici un message signé par le corsaire malouin Duguay-Trouin, chiffré par transposition (avec *padding* par le caractère `X`). Saurez-vous le déchiffrer ?

```
IFSSI LUNJN UMESS RAEEL EDTXS UEESA AXESR ESGDO CLDNC OUUDR LTDNY XRAET REGI
```

1. Donnez les différentes tailles possibles de la permutation. Puis en analysant la position des paddings, déduire la taille de la clé.
2. Terminez le déchiffrement du texte.

## Exercice 4 – Arithmétique modulaire et fonction indicatrice d'Euler – 5+3,5 points

Dans tout l'exercice, on note $\varphi$ la fonction indicatrice d'Euler. On rappelle que $\varphi(n)$ est le nombre d'entiers $a \in \{0, \ldots, n-1\}$ premiers avec $n$.

1. (**1 point**) Calculer $17^{2019} \bmod 36$.
2. (**0,5 point**) Soient $p$ un nombre premier. Montrer que $\varphi(p) = p - 1$.
3. (**0,5 point**) Soient $p$ un nombre premier et $e$ un entier non nul. Montrer que $\varphi(p^e) = p^e - p^{e-1}$.
4. (**1 point**) On suppose dans cette question que si $s$ et $t$ sont deux entiers premiers entre eux, alors $\varphi(s\,t) = \varphi(s)\,\varphi(t)$.
   Montrer que si $n = p_1^{e_1} \cdots p_r^{e_r}$ avec les $p_i$ des nombres premiers distincts deux à deux et les $e_i$ des entiers strictement positifs, alors $\varphi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdots \left(p_r^{e_r} - p_r^{e_r-1}\right) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$.
5. (**2 points**) À l'aide du résultat précédent, calculer $11^{43\,203} \bmod 189\,000$.
   *Les questions suivantes sont en bonus.*
   *Leur but est de prouver le résultat admis à la question 4, c'est-à-dire que si $s$ et $t$ sont premiers entre eux, alors $\varphi(s\,t) = \varphi(s)\,\varphi(t)$.*
6. (**1,25 point**) Soient $s$ et $t$ deux entiers premiers entre eux. Montrer que pour $a \in \{0, \ldots, t-1\}$ et $b \in \{0, \ldots, s-1\}$, les entiers $m_{a,b} = a\,s + b\,t \bmod s\,t$ sont tous distincts deux à deux. En déduire que pour tout entier $m$, $0 \leqslant m < s\,t$, il existe $a$ et $b$ comme précédemment tel que $m = a\,s + b\,t \bmod s\,t$.
7. (**1 point**) Montrer que pour $s$ et $t$ premiers entre eux, $\text{pgcd}(a, t) > 1$ ou $\text{pgcd}(b, s) > 1$ si, et seulement si, $\text{pgcd}(a\,s + b\,t, s\,t) > 1$.
8. (**0,5 point**) En déduire que si $a\,s + b\,t$ avec $a \in \{0, \ldots, t-1\}$ et $b \in \{0, \ldots, s-1\}$ est premier avec $s\,t$, alors $a$ est premier avec $t$ et $b$ est premier avec $s$.
9. (**0,75 point**) En déduire que le nombre de nombres $m \in \{0, \ldots, s\,t-1\}$ premiers avec $s\,t$ est $\varphi(s)\varphi(t)$.