Partiel de Cryptologie

13 mars 2019
Durée 1h45

Auteurs
Jérémy Berthomieu & Valérie Ménissier-Morain

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.

> **Solution :**
> Il s'agit d'appliquer successivement 2 opérations de chiffrements à un message clair pour en renforcer la sécurité. On peut utiliser le même cryptosystème, par exemple double Playfair ou double transposition (utilisés pendant la seconde guerre mondiale), ou bien 2 cryptosystèmes différents, par exemple ADFGVX avec substitution mono-alphabétique en utilisant le carré de Polybe suivi de transposition (utilisé pendant la première guerre mondiale).

2. (**3 points**) Quelles sont les solutions dans $\mathbb{Z}$ des équations : $4x + 2 = 5 \bmod 21$?

> **Solution :**
> 4 est premier avec 21 donc l'équation admet une infinité de solutions : $4 * 16 = 64 = 1 \bmod 21$ donc $4^{-1} = 16 \bmod 21$ et $x = 3 * 4^{-1} \bmod 21 = 6 \bmod 21$ donc $x = 6 + 21k$ pour tout $k \in \mathbb{Z}$.

$7x + 9 = 2 \bmod 21$? $3x + 1 = 2 \bmod 21$?

> **Solution :**
> 7 et 3 ne sont pas premiers avec 21 donc ne sont ni l'un ni l'autre inversible modulo 21. Il faut considérer les équations de plus près :
> — la première se réécrit $7x = -7 \bmod 21$. 7 divise à la fois 21 et le second membre de l'équation. Si x est solution de cette équation, il existe $k \in \mathbb{Z}$ tel que $7x = -7 + 21k$ ce qui est équivalent en divisant par 7 à $x = -1 + 3k$. Les solutions sont exactement les $x = -1 + 3k$ pour tout $k \in \mathbb{Z}$.
> — la seconde s'écrit $3x = 1 \bmod 21$. 3 ne divise pas 1 dans $\mathbb{Z}$ donc on ne peut pas diviser par 3 le membre droit de cette équation comme dans le cas précédent. 3 n'est pas inversible modulo 21 donc on ne peut pas non plus multiplier les deux membres de cette équation par son inverse comme dans le premier cas. Cette équation n'a pas de solution. On peut aussi dire que s'il existe une solution x alors $0 = 21x = 7 * (3x) = 7 * 1 = 7 \bmod 21$ ce qui est évidemment faux.

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.

Solution :
On va appliquer l'algorithme d'Euclide étendu à $a = 4541$ et $b = 3743$.
On utilise les notations usuelles, l'algorithme s'écrit

$$\begin{cases} u_0 = 1, & v_0 = 0, & r_0 = a \\ u_1 = 0, & v_1 = 1, & r_1 = b \\ u_{i+1} = u_{i-1} - q_i u_i, & v_{i+1} = v_{i-1} - q_i v_i, & r_{i+1} = r_{i-1} - q_i r_i \quad i \geqslant 1 \end{cases}$$

avec $q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor$ si $r_i \neq 0$ et sinon on s'arrête.
On a $r_i = u_i\, a + v_i\, b \ \ \forall i$.
On produit le tableau suivant :

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
					1	0
0	0	0	4541	3743	0	1
1	4541	1	3743	798	1	−1
2	3743	4	798	551	−4	5
3	798	1	551	247	5	−6
4	551	2	247	57	−14	17
5	247	4	57	19	61	−74
6	57	3	19	0	−197	239

On constate sur la 5ème ligne que $pgcd(a, b) = 19 \neq 1$ donc b n'est pas inversible modulo a. Sur la 6ème ligne on lit que $0 = -197a + 239b$ donc $239b = 0 \bmod a$ et 239 est un témoin de diviseur de 0 de $b = 3743$ dans $\mathbb{Z}/4541\mathbb{Z}$.

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.

Solution :
Ce sont les n qui sont premiers, soit $\{2, 3, 5\}$.
Ce sont les n qui sont des puissances d'un nombre premier, soit $\{2, 3, 4, 5\}$.

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 ?

Solution :
L'algorithme permert de résoudre le problème du logarithme discret dans G, c'est-à-dire trouver $k \in \{0, \cdots, |G| - 1\}$ tel que $h = g^k$ si G est engendré par g et $h \in G$. Sa complexité est en $O(\sqrt{|G|})$.

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`.

Solution :
On écrit le texte sur 3 colonnes puisque la clef a 3 caractères :

```
FUB
HTF
DNC
PCF
AE
```

On écrit la table de décalage pour chaque colonne :

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
--------------------------
PQRSTUVWXYZABCDEFGHIJKLMNO
ABCDEFGHIJKLMNOPQRSTUVWXYZ
XYZABCDEFGHIJKLMNOPQRSTUVW
```

ce qui donne

```
QUE
STI
ONF
ACI
LE
```

soit `Question facile`.

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.

Solution :

On voit que le texte chiffré comporte 64 caractères. La longueur ℓ de la transposition est donc un diviseur de 64, c'est-à-dire une puissance de 2 entre $2^0 = 1$ et $2^6 = 64$. Le nombre de colonnes est $64/\ell$.

On trouve 3 `X` en position 24, 32 et 56. Il y a donc un certain nombre de colonnes entières qui se terminent en position 24, 32 et 56 donc $64/\ell$ divise ces 3 nombres et leur $\text{pgcd}(24, 32, 56) = 8$ donc $\ell \geqslant 8$. On sait que les colonnes qui se terminent par `X` sont les trois dernières mais on ne peut en déduire l'ordre pour l'instant.

Il est temps de tirer parti de la signature : Duguay-Trouin. Pour pouvoir reconstituer l'ordre des colonnes, il faut qu'il n'y ait aucune ambiguïté. Or, en partant de la fin au-delà du 8e caractère on retombe sur le caractère `U` de `GUAY` qu'on a déjà rencontré dans `TROUIN`. Il nous faut impérativement ne pas dépasser 8 colonnes si nous voulons pouvoir reconstituer à coup sûr le texte clair sans élaborer d'hypothèse, on doit donc avoir $\ell \leqslant 8$.

Par conséquent $\ell = 8$.

2. Terminez le déchiffrement du texte.

Solution :
On écrit le texte sur 8 colonnes :

```
IJASECDR
FNEUSLRA
SUEERDLE
SMLEENTT
IEESSCDR
LSDAGONE
USTADUYG
NRXXOUXI
```

On identifie que les colonnes en position 3, 4 et 7 se terminent par `X` donc sont les dernières colonnes du texte avant transposition. Le texte comportait donc 64-3=61 caractères.

D'autre part le message est signé Duguay-Trouin, le texte clair en colonnes devait donc se terminer par

```
 DUGUAYT
ROUINXXX
```

La signature couvre donc avant transposition les colonnes 1 à 5 de la dernière ligne (`ROUIN`) et les colonnes 2 à 8 de l'avant-dernière ligne (`DUGUAYT`). On doit donc lire la colonne 2 (`R`) puis la colonne 5 (`O`), la colonne 6 (`U`), la colonne 8 (`I`) pour finir par la colonne 1 (`N`) pour replacer `ROUIN` dans la bonne position, c'est-à-dire au début de la dernière ligne avant les `XXX` de padding. Pour terminer il nous faut déplacer les colonnes restantes pour lire `AYT` dans les 3 dernières colonnes de l'avant-dernière ligne. On lit donc les colonnes 4, 7 et 3 pour terminer.

On a donc obtenu la permutation [2, 5, 6, 8, 1, 4, 7, 3] qu'on applique au texte :

```
JECRISDA
NSLAFURE
URDESELE
MENTSETL
ESCRISDE
SGOELAND
SDUGUAYT
ROUINXXX
```

qu'on relit en suite ligne à ligne :

```
JECRISDANSLAFUREURDESELEMENTSETLESCRISDESGOELANDSDUGUAYTROUIN
```

soit

```
J'écris dans la fureur des éléments et les cris des goélands. Duguay-Trouin
```

La permutation appliquée pour chiffrer, inverse de celle que nous venons d'appliquer pour déchiffrer, était [5, 1, 8, 6, 2, 3, 7, 4], qui permet d'ordonner en ordre alphabétique les caractères du mot `CORSAIRE`.

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

Dans tout l'exercice, on note φ 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} mod 36.

Solution :
On remarque que $17^2 = 289 = 8 * 36 + 1 = 1 \bmod 36$ donc $17^{2018} = 1 \bmod 36$ et $17^{2019} = 17 \bmod 36$.
Alternativement, $\varphi(36) = 12$ et 17 est premier avec 36 donc $17^{12} = 1$ et $17^{2019} = 17^{168\times12+3} = 17^3 = 17 \bmod 36$.

2. (**0,5 point**) Soient p un nombre premier. Montrer que $\varphi(p) = p - 1$.

Solution :
Clairement, 0 n'est pas premier avec p. De plus, comme p est premier, alors tout entier a tel que $0 < a < p$, a est premier avec p. Il y a donc $p - 1$ nombres a premiers avec p et $\varphi(p) = p - 1$.

3. (**0,5 point**) Soient p un nombre premier et e un entier non nul. Montrer que $\varphi(p^e) = p^e - p^{e-1}$.

Solution :
Si $0 \leqslant a < p^e$ n'est pas premier avec p^e, alors il admet un diviseur commun avec p^e supérieur à 1. Or p^e n'admet que des puissances de p comme diviseurs, donc a admet p comme diviseur. Or, les nombres strictement inférieurs à p^e divisibles par p sont exactement les $k\,p$ avec $k < p^{e-1}$ et il y en a donc p^{e-1}.
Il u a donc $p^e - p^{e-1}$ nombres a premiers avec p^e donc $\varphi(p^e) = p^e - p^{e-1} = p^e \left(1 - \frac{1}{p}\right)$.

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 $\varphi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdots \left(p_r^{e_r} - p_r^{e_r-1}\right) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$.

Solution :
Par récurrence immédiate sur r.
Le résultat est vrai pour $r = 1$ d'après la question précédente.
Supposons à présent que l'égalité soit vraie pour $r \geqslant 1$. Soit $n = p_1^{e_1} \cdots p_{r+1}^{e_{r+1}}$ un nombre avec $r + 1$ facteurs premiers, alors on écrit n sous la forme $n = s\,p_{r+1}^{e_{r+1}}$ avec s et $p_{r+1}^{e_{r+1}}$ premiers entre eux. D'après la formule admise dans l'énoncé, $\varphi(n) = \varphi(s)\,\varphi(p_{r+1}^{e_{r+1}})$ avec $\varphi(s) = \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdots \left(p_r^{e_r} - p_r^{e_r-1}\right)$ d'après l'hypothèse de récurrence et $\varphi(p_{r+1}^{e_{r+1}}) = \left(p_{r+1}^{e_{r+1}} - p_{r+1}^{e_{r+1}-1}\right)$ d'après la question précédente donc $\varphi(n) = \varphi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdots \left(p_{r+1}^{e_{r+1}} - p_{r+1}^{e_{r+1}-1}\right)$ et l'égalité est vraie aussi pour $r + 1$.
Par conséquent la propriété est vraie pour tout $r \in \mathbb{N}^*$.

5. (**2 points**) À l'aide du résultat précédent, calculer $11^{43\,203} \bmod 189\,000$.

Solution :
Clairement $n = 189\,000 = 189 \times 10^3 = 189 \times 2^3 \times 5^3$. De plus $189 = 3^3 \times 7$ donc $189\,000 = 2^3 \times 3^3 \times 5^3 \times 7$.
Ainsi $\varphi(n) = (2^3 - 2^2)\,(3^3 - 3^2)\,(5^3 - 5^2)\,(7 - 1) = 4 \times 18 \times 100 \times 6 = 43\,200$.
Comme 11 est premier avec n, alors d'après le théorème d'Euler $11^{\varphi(n)} = 1 \bmod n$, d'où $11^{43\,203} = 11^3 = 1\,331 \bmod n$.

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 $m = a\,s + b\,t \bmod s\,t$.

Solution :
Si (a, b) et (c, d) sont tels que $m_{a,b} = m_{c,d}$, alors $(a - c)\,s = (d - b)\,t \bmod s\,t$ et donc $(a - c)\,s = (d - b)\,t + k\,s\,t$ pour un certain $k \in \mathbb{Z}$. Comme s et t sont premiers entre eux, s divise $-s < d - b < s$ donc $d - b = 0$. Idem, $a - c = 0$. Par conséquent les couples $m_{a,b}$ pour $(a, b) \in \{0, \ldots, t-1\} \times \{0, \ldots, s-1\}$ sont tous distincts deux à deux.
Il y a $s\,t$ couples (a, b) dans cet ensemble. Il y a $s\,t$ entiers m tels que $0 \leqslant m < s\,t$ donc par le principe des tiroirs pour chaque entier m, il existe un unique couple (a, b) tel que $m = m_{a,b}$.

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, $\text{pgcd}(a\,s + b\,t, s\,t) > 1$.

Solution :
Comme $\text{pgcd}(a, t)$ divise a et t, il divise à la fois $a\,s + b\,t$ et $s\,t$ et donc $\text{pgcd}(a\,s + b\,t, s\,t)$. Par conséquent si $\text{pgcd}(a, t) > 1$, alors $\text{pgcd}(a\,s + b\,t, s\,t) > 1$. Il en va bien sûr de même si $\text{pgcd}(b, s) > 1$.
Réciproquement, si $\text{pgcd}(a\,s + b\,t, s\,t) > 1$, alors il existe p premier divisant $a\,s + b\,t$ et $s\,t$. Il divise donc s ou t et sans perte de généralité, on peut supposer qu'il divise t. Comme p divise aussi $a\,s + b\,t$, alors il divise $a\,s$. Or, s et t sont premiers entre eux donc p est premier avec s et p divise a. Ainsi p divise $\text{pgcd}(a, t) \geqslant p$.

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.

Solution :
D'après la question précédente, par contraposée, $\text{pgcd}(a, t) = \text{pgcd}(b, s) = 1$ si, et seulement si, $\text{pgcd}(a\,s + b\,t, s\,t) = 1$.

9. (**0,75 point**) En déduire que le nombre de nombres $m \in \{0, \ldots, s\,t - 1\}$ premiers avec $s\,t$ est $\varphi(s)\varphi(t)$.

Solution :
Pour $m \in \{0, \ldots, s\,t - 1\}$, il existe un unique couple $(a, b) \in \{0, \ldots, t-1\} \times \{0, \ldots, s-1\}$ tel que $m = a\,s + b\,t \bmod s\,t$. De plus, m est premier avec $s\,t$ si, et seulement si, a est premier avec t et b avec s. Il y a donc $\varphi(t)$ possibilités pour a et $\varphi(s)$ pour b, d'où $\varphi(s)\varphi(t)$ pour le couple (a, b).