Partiel de Cryptologie

15 mars 2024
Durée 1h30

Auteurs
Valérie Ménissier-Morain & …

Version du 1er avril 2024

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

Exercice 1 – Chiffrement Parfait et Vigenère – 5 points

1. (**1 point**) Rappeler la définition du cryptosystème de Vigenère avec des clefs de longueur ℓ et agissant sur des blocs de même taille (vous préciserez l'ensemble des caractères en clair $\mathcal{P}$, l'ensemble des caractères chiffrés $\mathcal{C}$ et l'ensemble des clefs $\mathcal{K}$ en fonction de ℓ).

> **Solution :**
> $\mathcal{P} = \mathcal{C} = \mathcal{K} = A^\ell$, on chiffre le mot $m_1 \dots m_\ell$ avec la clef $k_1 \dots k_\ell$ en remplaçant la lettre m_i par $c_i = (m_i + k_i)$ mod $|A|$.

2. (**2 points**) Montrer que le cryptosystème de Vigenère ainsi défini est un chiffrement parfait.

> **Solution :**
> On a : $\mathcal{P} = \mathcal{C} = \mathcal{K} = A^\ell$, donc $\#P = \#C = \#K$, les clefs sont équiprobables de probabilité $1/|A|^\ell$ et pour tout couple $(m, c) \in P \times C$ avec $m = m_1 \dots m_\ell$ et $c = c_1 \dots c_\ell$, il existe une unique clef $k = k_1 \dots k_\ell$ avec $k_i = c_i - m_i$ telle que $e_k(m) = c$ donc d'après le théorème de caractérisation, le chiffrement est parfait.

3. (**2 points**) Supposons que les clefs secrètes soient tirées au hasard dans un des trois dictionnaires Larousse, Robert ou Littré (éditions 1863). En conservant les mêmes définitions pour $\mathcal{P}$ et $\mathcal{C}$ le chiffrement de la question précédente reste-t-il parfait ? Vous expliquerez votre réponse.

> **Solution :**
> Le cardinal de $\mathcal{K}$ est réduit maintenant et donc $\#\mathcal{K} < \#\mathcal{P}$, le chiffrement n'est plus parfait.

Exercice 2 – Algèbre et arithmétique – 9 points

1. (**2 points**) Soit n un entier naturel produit de deux nombres premiers distincts p et q. L'anneau $A = \mathbb{Z}/n\mathbb{Z}$ peut-il contenir des sous-groupes d'ordre p ou q ? En contient-il toujours de cet ordre ? Vous argumenterez soigneusement vos réponses.
   Donner un exemple de tels sous-groupes pour une valeur fixée de n.

   Solution :
   D'après le théorème de Lagrange l'ordre de tout sous-groupe de A divise n l'ordre de A . Or n est le produit de deux nombres premiers p et q donc possède seulement deux diviseurs propres p et q . Par conséquent l'ordre d'un sous-groupe strict de A ne peut être que p ou q .
   L'anneau $\mathbb{Z}/n\mathbb{Z}$ est cyclique quelle que soit la valeur de n . Soit g un générateur de A, alors $\langle g^q \rangle$ est un sous-groupe d'ordre p de A et $\langle g^p \rangle$ est un sous-groupe d'ordre q de A . A admet donc toujours des sous-groupes d'ordre p et q et ne peut pas contenir de sous-groupe strict d'ordre différent .

2. (**1 point**) Soit $p > 3$ un entier irréductible. Montrer que $p - 1$ ne peut pas être irréductible.

   Solution :
   Si $p > 3$ un entier irréductible, alors p est un nombre premier impair donc $p - 1$ est un nombre pair plus grand que 2 et n'est pas irréductible.

3. (**1 point**) Soit a un entier qui est un inverse modulo un autre entier n. Montrer que le pgcd de a et n est égal à 1.

   Solution :
   Ceci revient à montrer le corollaire du Théorème de Bézout . Puisque a est un inverse modulo n il existe u tel que $au = 1 \mod n$. Il existe donc v tel que $au + nv = 1$ dans $\mathbb{Z}$. Si d est un diviseur positif de a et n alors $a = da'$, $n = dn'$ et
   $$au + nv = da'u + dn'v = d(a'u + n'v) = 1$$
   Donc d divise 1 et le résultat suit.

4. (**3 points**) L'entier 239 est-il inversible ou un diviseur de zéro dans $\mathbb{Z}/684\mathbb{Z}$. S'il est inversible calculer l'entier $b \in \mathbb{Z}/684\mathbb{Z}$ tel que $239 \times b = 1 \mod 684$. Si c'est un diviseur de zéro calculer un entier $b \in \mathbb{Z}/684\mathbb{Z}$ non nul tel que $239 \times b = 0 \mod 684$.
   Quel algorithme utilisez-vous pour cela ?
   Vous donnerez l'ensemble des calculs intermédiaires (les différentes relations entre les quotients et restes successifs) sous la forme d'un tableau comme vu en cours ou en TD et vous expliquerez comment vous construisez votre tableau.

   Solution :
   On applique l'algorithme d'Euclide étendu à $a = 684$ et $n = 239$.
   Dans le tableau suivant chaque ligne à partir de la ligne $i = 1$ se lit :
   - la partie gauche (colorée en rose), si $r_i \neq 0$, la division euclidienne de r_{i-1} par r_i est $r_{i-1} = q_i * r_i + r_{i+1}$ qui définit le quotient $q_i = \lfloor \frac{r_{i-1}}{r_i} \rfloor$ et le reste suivant $r_{i+1} = r_{i-1} - q_i * r_i$; sinon on s'arrête.
   - pour la partie droite (colorée en jaune), $u_{i+1} = u_{i-1} - q_i * u_i$ et $v_{i+1} = v_{i-1} - q_i * v_i$
   - avec l'initialisation (partie en haut, colorée en bleu) : $r_0 = a$, $r_1 = b$, $u_0 = v_1 = 1$, $v_0 = u_1 = 0$
   - à chaque étape on a $r_i = u_i\, n + v_i\, a \ \ \forall i$.

   On exploite cette information sur les deux dernières lignes du tableau (cadres rouge et vert) :
   - avant-dernière ligne (de numéro k), on trouve r_{k+1} (dans la cinquième colonne) le dernier reste positif, c'est-à-dire le pgcd de n et a et $r_{k+1} = u_{k+1}\, n + v_{k+1}\, a$ est une relation de Bézout .
     Si $r_{k+1} = 1$, alors $v_{k+1} \mod n$ est l'inverse de a modulo n , a n'est pas diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$.

— à la dernière ligne (de numéro $k+1$ donc), on trouve $0 = r_{k+2} = n\,u_{k+2} + a\,v_{k+2}$.
Si $r_{k+1} > 1$, alors a n'est pas inversible modulo n, c'est un diviseur de 0 dans $\mathbb{Z}/n\mathbb{Z}$, $|v_{k+2}| < n$ donc v_{k+2} est un témoin de diviseur de 0 pour a dans $\mathbb{Z}/n\mathbb{Z}$.

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
-1					1	0
0			684	239	0	1
1	684	2	239	206	1	-2
2	239	1	206	33	-1	3
3	206	6	33	8	7	-20
4	33	4	8	1	-29	83
5	8	8	1	0	239	-684

Ici $k = 4$, on constate que $\text{pgcd}(a, n) = r_{k+1} = 1$ donc a est inversible modulo n d'inverse $v_{k+1} = 83$. 239 n'est pas diviseur de zéro pour 684.

5. (**2 points**) Quelle est la valeur de x pour laquelle $3x + 7 = 5 \bmod 13$? Idem pour $3x + 7 = 5 \bmod 12$?

Solution :
On peut réécrire l'équation $3x = 5-7 = -2 = 11 \bmod 13$ dans le premier cas et $3x = 5-7 = -2 = 10 \bmod 12$ dans le second cas .
Dans le premier cas 3 est premier avec 13 , d'inverse $3^{-1} = 9 \bmod 13$ puisque $3 * 9 = 27 = 1 \bmod 13$ (on pourrait évidemment utiliser l'algorithme d'Euclide étendu pour calculer cet inverse) , donc $x = 11 * 3^{-1} = 11 * 9 = 99 = 8 \bmod 13$ et on peut vérifier que $3x + 7 = 3 * 8 + 7 = 31 = 5 \bmod 13$.
Dans le second cas en revanche, $\text{pgcd}(3, 12) = 3$ et 3 ne divise pas 10 donc l'équation n'a pas de solution .

Exercice 3 – Vigenère sans modulo – 4 points

Alice et Bob n'ont pas été attentifs lors du cours de présentation du chiffrement de Vigenère. Ils essaient de communiquer de manière chiffrée mais utilisent une variante du chiffrement de Vigenère qui fonctionne de la manière suivante : pour chaque lettre du message, on calcule son rang dans l'alphabet (`A` = 0, `B` = 1, ...), et on l'ajoute au rang de la lettre correspondante dans la clef, comme pour le chiffrement Vigenère. Mais ils oublient de faire le calcul modulo 26.

Par exemple, le message `VIGENERESANSMODULO` chiffré avec la clef `CRYPTO` donne le message chiffré `23 25 30 19 32 18 19 21 42 15 32 32 14 31 27 35 30 28`, comme détaillé ci-dessous.

```
   V  I  G  E  N  E    R  E  S  A  N  S    M  O  D  U  L  O
  21  8  6  4 13  4   17  4 18  0 13 18   12 14  3 20 11 14
+  C  R  Y  P  T  O    C  R  Y  P  T  O    C  R  Y  P  T  O
   2 17 24 15 19 14    2 17 24 15 19 14    2 17 24 15 19 14
-------------------------------------------------------------
= 23 25 30 19 32 18   19 21 42 15 32 32   14 31 27 35 39 28
```

1. (**3 points**) Le message suivant a été chiffré avec une clef de longueur 3. Pouvez-vous retrouver le message et la valeur de la clef de chiffrement ?

`01 33 20 05 27 04 05 39 14 15 34 19 01 25 01 16 22 26 26 18 18 09 14 04 21 39 15 15`

Solution :
On reconstitue les colonnes de nombres du chiffré , ce qui donne :

```
01 33 20
05 27 04
05 39 14
15 34 19
01 25 01
16 22 26
26 18 18
09 14 04
21 39 15
15
```

On observe que :

— dans les colonnes 1 et 3 les nombres varient de 1 à 26. Ces nombres sont de la forme $d + p$ où d est le décalage et p est un caractère du texte clair donc correspond à un nombre compris entre 0 et 25 . On voit que le seul décalage possible est donc 1 ;

— dans la colonne 2 les nombres varient de 14 à 39. De la même façon on trouve que le seul décalage possible est 14.

En résumé notre clef chiffrée est `01 14 01` , ce qui correspond à la clef textuelle `Bob` et on déchiffre le texte :

```
  01 33 20 05 27 04 05 39 14 15 34 19 01 25 01 16 22 26 26 18 18 09 14 04 21 39 15 15
- 01 14 01 01 14 01 01 14 01 01 14 01 01 14 01 01 14 01 01 14 01 01 14 01 01 14 01 01
------------------------------------------------------------------------------------
  00 19 19 04 13 03 04 25 13 14 20 18 00 11 00 15 08 25 25 04 17 08 00 03 20 25 14 14
   A  T  T  E  N  D  E  Z  N  O  U  S  A  L  A  P  I  Z  Z  E  R  I  A  D  U  Z  O  O
```

soit *Attendez-nous à la pizzeria du zoo*.

2. (**1 point**) Expliquez la faiblesse de ce mode de chiffrement.

Solution :
En l'absence de modulo, l'ensemble des lettres chiffrées avec la même clé est à valeurs dans l'intervalle $[0; 25]$ décalé de la valeur de la clé. Cela permet donc de réduire les valeurs possibles pour chacune des clés, à partir du moment où la longueur est connue. Pour déterminer la longueur, on peut utiliser, comme pour le chiffrement de Vigenère classique, l'indice de coincidence, avec en plus la contrainte que pour une sous-clé fixée, il ne peut y avoir qu'un écart de 25 au maximum.

Exercice 4 – Chiffrement nihiliste – 9 points

Dans cet exercice, l'alphabet des messages clairs $\mathcal{P}$ est l'alphabet à 25 lettres, qui correspond à l'alphabet français sans la lettre `W` (si on veut chiffrer un `W` on le remplace par `V`). L'alphabet des chiffrés est $\mathcal{C}$.

La clef consiste en deux chaînes de caractères, qu'on appellera (K_1, K_2). Pour chiffrer, on procède en deux étapes.

1 – Utilisation de K_1 :

On part d'un carré 5×5 dont les lignes et colonnes sont numérotées de 0 à 4. On le remplit de gauche à droite et de haut en bas, d'abord avec les lettres de la clef K_1 (sans les répéter), puis en complétant avec les lettres restantes de l'alphabet $\mathcal{P}$. Par exemple, si la clef K_1 est `CRYPTOGRAPHIE` on obtient le carré suivant :

	0	1	2	3	4
0	C	R	Y	P	T
1	O	G	A	H	I
2	E	B	D	F	J
3	K	L	M	N	Q
4	S	U	V	X	Z

On repère un caractère de l'alphabet $\mathcal{P}$ par ses coordonnées (ligne et colonne) dans ce tableau. Par exemple la lettre `B` est représentée par `21` pour cette clef K_1.

1. (**1 point**) Combien existe-t-il de carrés possibles ?

Solution :
Il y a 25 cases, il y a autant de carrés possibles que de permutations du contenu de ces 25 cases, soit 25 !

2 – Utilisation de K_2 :

Après avoir remplacé chaque lettre du message par ses coordonnées dans le carré déterminé par K_1 et fait de même pour chaque lettre de K_2, on applique un chiffrement de Vigenère avec la clef K_2 sans modulo. Le chiffré est donc composé de chiffres de 0 à 8 : $\mathcal{C} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.

Par exemple, avec la clef (CRYPTOGRAPHIE, ALKINDI), c'est-à-dire avec le carré ci-dessus et K_2 = ALKINDI, si l'on souhaite chiffrer le message BONCOURAGEPOURLEPARTIEL, on obtient :

```
   B  O  N  C  O  U  R    A  G  E  P  O  U  R    L  E  P  A  R  T  I    E  L
  21 10 33 00 10 41 01   12 11 20 03 10 41 01   31 20 03 12 01 04 14   20 31
+  A  L  K  I  N  D  I    A  L  K  I  N  D  I    A  L  K  I  N  D  I    A  L
  12 31 30 14 33 22 14   12 31 30 14 33 22 14   12 31 30 14 33 22 14   12 31
-------------------------------------------------------------------------------
= 33 41 63 14 43 63 15   24 42 50 17 43 63 15   43 51 33 26 34 26 28   32 62
```

2. (**2 points**) Chiffrez le message RDVDEMAINSOIR avec la clef K_1 = VIGENERE et K_2 = ALICE. Commencez par expliciter le carré obtenu à partir de la clef K_1.

Solution :

Le carré associé à K_1 =VIGENERE :

	0	1	2	3	4
0	V	I	G	E	N
1	R	A	B	C	D
2	F	H	J	K	L
3	M	O	P	Q	S
4	T	U	X	Y	Z

K_2 =ALICE a pour équivalent numérique selon ce carré 11 24 01 13 03, d'où le chiffré du message RDVDEMAINSOIR :

```
   R  D  V  D  E    M  A  I  N  S    O  I  R
  10 14 00 14 03   30 11 01 04 34   31 01 10
+  A  L  I  C  E    A  L  I  C  E    A  L  I
  11 24 01 13 03   11 24 01 13 03   11 24 01
-----------------------------------------------
= 21 38 01 27 06   41 35 02 17 37   42 25 11
```

3. (**1 point**) Vous avez reçu la réponse 23 25 04 17 13 14 37 42 24 17 14 54 12 14 07 au message précédent. Cette réponse a été chiffrée avec les mêmes clefs. Déchiffrez ce message.

Solution :

```
  23 25 04 17 13   14 37 42 24 17   14 54 12 14 07
- 11 24 01 13 03   11 24 01 13 03   11 24 01 13 03
-------------------------------------------------
= 12 01 03 04 10   03 13 41 11 14   03 30 11 01 04
   B  I  E  N  R    E  C  U  A  D    E  M  A  I  N
```

soit Bien reçu. À demain.

4. (**1 point**) Est-ce que tous les éléments de l'alphabet du chiffré $\mathcal{C}$ apparaissent avec la même fréquence ? Justifiez votre raisonnement.

Solution :

L'alphabet du chiffré est l'ensemble des chiffres de 0 à 8.

La seconde étape est une somme sans modulo, ce qui biaise la distribution, en particulier pour les valeurs extrêmes : un 0 n'apparait que si la clé et le chiffré intermédiaire valent 0 à cet endroit, un 8 n'apparait que si les

deux valent 4, alors qu'il y a 6 façons différentes d'obtenir 5 : 5+0, 4+1, 3+2, 2+3, 1+4, 0+5 .

5. (**4 points**) Ève écoute les échanges chiffrés entre Alice et Bob. Ce matin, elle a intercepté un nouveau message :

```
35 50 75 20 34 84 84 33 27 42 84 10 56 60 54 10 44 64
63 10 65 41 75 40 37 50 55 13 27 54 63 10 54 41 87 44
```

Grâce à son réseau d'espions, Ève a obtenu les informations suivantes :
— Ce message contient le lieu de la prochaine rencontre d'Alice et Bob. Par conséquent, le message doit sûrement commencer par `RENDEZVOUS`.
— Alice et Bob choisissent toujours une clé avec K_2 de longueur 4.
— Ève a réussi à récupérer une partie du carré utilisé pour le chiffrement :

	0	1	2	3	4
0	M			U	
1			C		B
2					
3			N		
4	T		X		

Saurez-vous déchiffrer le message à l'aide de ces informations ?

Solution :
Puisque K_2 a 4 caractères, nous allons écrire le message sur 4 colonnes :

```
35 50 75 20
34 84 84 33
27 42 84 10
56 60 54 10
44 64 63 10
65 41 75 40
37 50 55 13
27 54 63 10
54 41 87 44
```

On s'intéresse pour chaque chiffre à l'amplitude couverte :
1. entre `2` et `6`, ce qui montre que le décalage est de `2` ;
2. entre `4` et `7`, ce qui laisse deux possibilités : un décalage de `3` ou de `4` ;
3. entre `4` et `8`, ce qui montre que le décalage est de `4` ;
4. entre `0` et `4`, ce qui montre que le décalage est de `0` ;
5. entre `5` et `8`, ce qui montre que le décalage est de `4` ;
6. entre `3` et `7`, ce qui montre que le décalage est de `3` ;
7. entre `1` et `4`, ce qui laisse deux possibilités : un décalage de `0` ou de `1` ;
8. entre `0` et `4`, ce qui montre que le décalage est de `0`.

En résumé la version numérique de K_2 est `2(3|4) 40 43 (0|1)0`.

Nous connaissons le caractère en position `40` dans le tableau, c'est `T`.
Nous déduisons du `X` en position `42` qu'en positions `41`, `43` et `44` se trouvent respectivement les caractères `V`, `Y` et `Z` qui terminent l'alphabet.
La clef K_2 comporte donc soit le caractère en position `23` soit celui en position `24` puis `TY` et ensuite le caractère en position `00` (`M`) ou celui en position `01`.
Nous avons exploité tout ce que nous avons trouvé pour l'instant comme information pour la clef K_2. Nous allons nous intéresser au déchiffrement du chiffré pour cette étape en soustrayant `23` ou `24` à la première colonne, `40` à la deuxième, `43` à la troisième puis `00` ou `10` à la dernière :

24 ou 23	40	43	10 ou 00
11 ou 12	10	32	10 ou 20
10 ou 11	44	41	23 ou 33
03 ou 04	02	41	00 ou 10
32 ou 33	20	11	00 ou 10
20 ou 21	24	20	00 ou 10
41 ou 42	01	32	30 ou 40
13 ou 14	10	12	03 ou 13
03 ou 04	14	20	00 ou 10
30 ou 31	01	44	34 ou 44

et en lettres

24 ou 23	40	43	10 ou 00
_ ou C	_	N	_ ou _
_ ou _	Z	V	_ ou _
U ou _	_	V	M ou _
N ou _	_	_	M ou _
_ ou _	_	_	M ou _
V ou X	_	N	_ ou T
_ ou B	_	C	U ou _
U ou _	B	_	M ou _
_ ou _	_	Z	_ ou Z

Il nous reste une information que nous n'avons pas encore exploité : le message contient `RENDEZVOUS`. Or il est tout à fait possible de caser `RENDEZVOUS` au début du texte car tous les caractères connus de façon sûre coïncident. Cela nous donne une pluie d'informations :

- le premier décalage est `24`, la première lettre est `R` et numériquement `11`
- la deuxième lettre, numériquement `10` est un `E`
- le dernier décalage est `00`, la dernière lettre est `D` et numériquement `20`
- la dernière lettre de la deuxième ligne est un `O`, numériquement `33`
- la deuxième lettre de la troisième colonne est un `S`, numériquement `02`.

Il est temps de reporter ces informations sur K_2 =`24 40 43 00=?TYM` et sur le carré associé à K_1

	0	1	2	3	4
0	M		S	U	
1	E	R	C		B
2	D				
3			N	O	
4	T	V	X	Y	Z

et sur le message

11	10	32	20		R	E	N	D
10	44	41	33		E	Z	V	O
03	02	41	10		U	S	V	E
32	20	11	10		N	D	R	E
20	24	20	10	et en lettres	D	_	D	E
41	01	32	40		V	_	N	T
13	10	12	13		_	E	C	_
03	14	20	10		U	B	D	E
30	01	44	44		_	_	Z	Z

On devine que la lettre `24` correspond à `I`, la lettre `01` correspond à `A`, la lettre `13` correspond à `L` et finalement la lettre `30` correspond à `J`. Cela nous donne le message `RENDEZVOUSVENDREDIDEVANTLECLUBDEJAZZ`, plus clairement *Rendez-vous vendredi devant le club de jazz*. Le carré associé à K_1 est

	0	1	2	3	4
0	M	A	S	U	P
1	E	R	C	L	B
2	D	F	G	H	I
3	J	K	N	O	Q
4	T	V	X	Y	Z

K_1 =`MASUPERCLE` (ou `MASUPERCLASSE` il n'y a pas unicité à partir du carré de Polybe) et K_2 =`ITYM`. Nous avons réussi à déchiffrer le message.