TD Cryptographie et sécurité

Congruences

Exercice 1

Inverse modulo n

Déterminer si l'inverse des éléments suivants existe dans $\mathbb{Z}/27\mathbb{Z}$. Si c'est le cas, préciser l'inverse avec un représentant dans $[\![0,\ 26]\!]$.

1. $\overline{18}$,
2. $\overline{14}$.

Indications

- $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $PGCD(a, n) = 1$.
- L'algorithme d'Euclide permet alors de déterminer l'inverse s'il existe.

Exercice 2

Petit théorème de Fermat

1. Montrer $2^6 \equiv 1 \pmod 7$.
2. En déduire $2^{3\,000} \equiv 1 \pmod 7$, puis $7|2^{3\,000} - 1$.
3. Montrer que le nombre premier $3\,001$ divise $2^{3\,000} - 1$.
4. Montrer $2^3 \equiv -1 \pmod 9$.
5. En déduire $2^{3\,000} \equiv 1 \pmod 9$, puis $9|2^{3\,000} - 1$.
6. Déduire des questions précédentes $189\,063 = 3^2 \times 7 \times 3\,001$ divise $2^{3\,000} - 1$.

Exercice 3

Théorème du reste chinois

1. Résoudre dans $\mathbb{Z}$: $\begin{cases} x \equiv 7 \,(\mathrm{mod}\, 11) \\ x \equiv 4 \,(\mathrm{mod}\, 19) \end{cases}$
2. **Problème du cuisinier prisonnier**
   Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager et de donner le reste au cuisinier prisonnier. Celui-ci recevrait alors trois pièces. Mais les pirates se querellent et six d'entre eux sont tués. Le cuisinier recevrait alors quatre pièces. Dans un naufrage ultérieur, seuls le butin, six pirates et le cuisinier sont sauvés et le partage laisserait cinq pièces d'or à ce dernier. Quelle est alors la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates ?

Cryptographie asymétrique

Exercice 4

Chiffrement RSA (Rivest, Shamir et Adleman)

1. **Codage des caractères alphabétiques**
   A chaque lettre x de l'alphabet, on associe son rang $r(x)$ dans l'alphabet de la manière suivante.

x	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
r(x)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

   On découpe le message en "mots" de trois caractères xyz auxquels on associe le nombre $r(x) \times 26^2 + r(y) \times 26 + r(z)$.
   Exemple : ARC est codé $r(A) \times 26^2 + r(R) \times 26 + r(C) = 0 + 17 \times 26 + 2 = 444$.
   On peut ensuite décoder un mots de trois caractères par divisions successives par 26.
   Exemple : $11\,864 = 456 \times 26 + 8$ et $456 = 17 \times 26 + 14$ conduisent à : $11\,864 = 17 \times 26^2 + 14 \times 26 + 8$, qui permet de voir que 11 864 code le mot ROI.

2. **Méthode RSA**
   Résultats fondant la méthode
   Soient p et q des entiers premiers, a un entier non multiple de p et non multiple de q, c un entier premier avec $(p-1)(q-1)$.
   On démontre

   - Il existe un entier d tel que $cd \equiv 1 \pmod{(p-1)(q-1)}$.
   - $(a^c)^d \equiv a \pmod{pq}$.

   Démonstration
   - Comme c est premier avec $(p-1)(q-1)$, $\overline{c}$ est inversible dans $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$. Il existe donc un entier d tel que $cd \equiv 1 \pmod{(p-1)(q-1)}$ et alors un entier k tel que $cd = 1 + k(p-1)(q-1)$.
   - En utilisant le petit théorème de Fermat, $a^{(p-1)} \equiv 1 \pmod{p}$ et $a^{(q-1)} \equiv 1 \pmod{q}$. On en déduit alors $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.
   - On obtient ensuite $(a^c)^d = a^{cd} = a^{1+k(p-1)(q-1)} = a\left(a^{(p-1)(q-1)}\right)^k \equiv a \times 1^k \equiv a \pmod{pq}$.

   Méthode
   Supposons qu'un enseignant X souhaite recevoir un message chiffré d'un enseignant Y. X choisit deux nombres premiers p et q, calcule $n = pq$ et $m = (p-1)(q-1)$. Il choisit ensuite un entier c premier avec m, puis détermine d tel que $cd \equiv 1 \pmod{m}$. X communique ensuite n et c à Y.
   Si Y veut adresser un message chiffré à X, il le transforme en séries de nombres correspondant à des mots de trois lettres, puis pour chacun de ces nombres a, il calcule $a^c \pmod{n}$, qu'il communique à X. Celui-ci déchiffrera chacun de ces nombres en calculant $(a^c)^d \equiv a \pmod{n}$.

   Exemple
   X choisit $p = 127$, $q = 131$.
   On a donc $n = pq = 16\,637$ et $m = (p-1)(q-1) = 16\,380 = 2^2 \times 3^2 \times 5 \times 7 \times 13$.
   X choisit ensuite $c = 11.23 = 253$ qui est bien premier avec m. Il calcule ensuite d tel que $cd \equiv 1 \pmod{m}$ et il obtient grâce à l'algorithme d'Euclide :

r	u	v	q
16 380	1	0	
253	0	1	64
188	1	-64	1
65	-1	65	2
58	3	-194	1
7	-4	259	8
2	35	-2266	3
1	-109	7057	2
0			

$16\,380 \times (-109) + 253 \times 7\,057 = 1$ conduit à $253 \times 7\,057 \equiv 1 \pmod{16\,380}$ et donc à $d = 7\,057$.
X communique n et c à Y.
Supposons que Y veuille adresser le message ROI à X. Il le transforme d'abord en 11 864 comme décrit ci-dessus, puis vérifie que 11 864 est premier avec $n = 16\,637$: $PGCD(11\,864, 16\,637) = 1$.
Il calcule ensuite $11\,864^{253} \pmod{16\,637}$, et envoie le message chiffré 9 832 à X. Ce dernier calcule alors $9\,832^{7\,057} \pmod{16\,637}$, obtient 11 864 (mod 16 637) et lit le mot ROI.

Remarques

(a) Un entier n produit de deux nombres premiers impairs est appelé un module RSA.

(b) $m = (p-1)(q-1)$ est aussi noté $\phi(n)$ (fonction indicatrice d'Euler : le nombre d'entiers compris entre 1 et n et premiers avec n).

(c) a est compris entre 0 et $25 \times 26^2 + 25 \times 26 + 25 = 17\,575$. Pour que a ne soit ni un multiple de p ni un multiple de q, on prend p et q supérieurs à 17 576.

(d) La méthode RSA est d'autant plus sûre que la factorisation de n en produit de deux nombres premiers p et q est difficile. Actuellement les algorithmes de factorisation peuvent factoriser en un temps raisonnable des nombres d'au plus 150 chiffres. On prend donc des nombres p et q de l'ordre de 100 chiffres pour que n ait de l'ordre de 200 chiffres.

(e) En fait, X peut communiquer les nombres n et c à tous les gens susceptibles de lui adresser des messages chiffrés par cette méthode, puisqu'il est le seul à pouvoir les déchiffrer. On dit que la méthode RSA est à clé publique. n et c constituent la clé publique qu'on note aussi (c,n). Le couple (d,n) est appelé clé privée ou secrète.

(f) Se pose le problème du calcul effectif des nombres a^c et $(a^c)^d \pmod{n}$. Pour le calcul de $a^c \pmod{n}$, on écrit c en base 2, et on calcule les carrés des carrés successifs (exponenciation modulaire par carré).

(g) Le calcul de $a \pmod{b}$ avec une calculatrice peut se faire en utilisant $a = b \times q + r$ $(0 \leq r < b)$, $q = \left[\frac{a}{b}\right]$ car $0 \leq \frac{a}{b} - q < 1$ et $r = \left(\frac{a}{b} - \left[\frac{a}{b}\right]\right) \times b$.

Exemple

Pour calculer $11\,864^{253} \pmod{16\,637}$, on écrit 253 en base 2 :
$253 = 1 + 0 \times 2^1 + 1 \times 2^2 + 1 \times 2^3 + 1 \times 2^4 + 1 \times 2^5 + 1 \times 2^6 + 1 \times 2^7$
soit $253 = 1 + 4 + 8 + 16 + 32 + 64 + 128$.
On a donc $a^{253} = a^{1+4+8+16+32+64+128} = a \times a^4 \times a^8 \times a^{16} \times a^{32} \times a^{64} \times a^{128}$.
On calcule ensuite modulo 16 637 :
$a = 11\,864$
$a^2 = 11\,864^2 = 140\,754\,496 \equiv 5\,476$

$a^4 \equiv 5\,476^2 = 29\,986\,576 \equiv 6\,702$
$a^8 \equiv 6\,702^2 = 44\,916\,804 \equiv 13\,541$
$a^{16} \equiv 13\,541^2 = 183\,358\,681 \equiv 2\,304$
$a^{32} \equiv 2\,304^2 = 5\,308\,416 \equiv 1\,213$
$a^{64} \equiv 1\,213^2 = 1\,471\,369 \equiv 7\,313$
$a^{128} \equiv 7\,313^2 = 53\,479\,969 \equiv 8\,651$.
On en déduit en calculant le produit de proche en proche modulo 16 637 :
$11\,864 \times 6\,702 = 79\,512\,582 \equiv 4\,305$
$4\,305 \times 13\,541 = 58\,294\,005 \equiv 14\,594$
$14\,594 \times 2\,304 = 33\,624\,576 \equiv 1\,199$
$1\,199 \times 1\,213 = 1\,454\,387 \equiv 6\,968$
$6\,968 \times 7\,313 = 50\,956\,984 \equiv 14\,490$
$14\,490 \times 8\,651 = 125\,352\,990 \equiv 9\,832$
$11\,864^{253} \equiv 9\,832 \pmod{16\,637}$

3. **Questions**

   (a) X a choisi $p = 107$ et $q = 137$. Il a donc $n = 107 \times 137 = 14\,659$ et $m = 106 \times 136 = 14\,416 = 2^4 \times 17 \times 53$.
   X choisit ensuite $c = 3^2 \times 5 \times 13 \times 23 = 13\,455$ (premier avec m) et en déduit d tel que $cd \equiv 1 \pmod{m}$.

   i. Déterminer d.

   ii. X communique (c, n) à Y.
   Ce dernier chiffre un message selon la méthode RSA et l'adresse à X qui reçoit : 9 633.
   Déchiffrer ce message. Le décoder.

   (b) X a choisi $p = 97$, $q = 149$ et $c = 17$.

   i. Préciser $n = pq$ et $m = (p-1)(q-1)$.

   ii. Vérifier que c est premier avec m.

   iii. Déterminer d tel que $cd \equiv 1 \pmod{m}$.

   iv. X communique (c, n) à Y.
   Y souhaite chiffrer le message : IUT et l'adresser à X.
   Coder le message et vérifier que le nombre a obtenu est premier avec n.

   v. Chiffrer a.

Exercice 5

Cryptanalyse RSA connaissant m

1. Montrer que si on connaît $n = pq$ et $m = (p-1)(q-1)$, $p < q$, alors on peut factoriser n.
   Indication : en posant $S = x_1 + x_2$ et $P = x_1 x_2$, x_1 et x_2 sont solutions de $x^2 - Sx + P = 0$.
2. Application numérique : $n = 1\,073$, $m = 1\,008$.

Remarque

L'algorithme de Héron permet la détermination de $\sqrt{a}$. Il est défini par $u_{n+1} = \frac{1}{2}\left(u_n + \frac{a}{u_n}\right)$

et $u_0 > 0$ (u_0 peut être une valeur approchée de $\sqrt{a}$).
De manière plus générale, un algorithme de détermination de la racine k-ième de a : $\sqrt[k]{a}$ est défini par $u_{n+1} = \frac{1}{k}\left((k-1)u_n + \frac{a}{u_n^{k-1}}\right)$ et $u_0 > 0$ (u_0 peut être une valeur approchée de $\sqrt[k]{a}$).
Il s'agit d'une application de la méthode de Newton s'appliquant à la fonction $f(x) = x^k - a$: $u_{n+1} = u_n - \frac{f(u_n)}{f'(u_n)}$. L'algorithme de Héron est un cas particulier de la méthode de Newton.
Héron d'Alexandrie : mathématicien grec du Ier siècle après Jésus Christ.
Isaac Newton ($1\,642 - 1\,727$) : mathématicien, physicien, philosophe, alchimiste, astronome et théologien anglais.

Exercice 6

Cryptanalyse RSA utilisant le même module n
Soit n un module RSA.

1. Montrer qu'un message clair a chiffré avec c_1 et c_2 premiers entre eux peut être déchiffré sans factoriser le module n.
   Indication
   On note C_1 et C_2 les messages chiffrés à partir du même message clair a avec les clés publiques (c_1, n) et (c_2, n) : $C_1 \equiv a^{c_1} \pmod{n}$ et $C_2 \equiv a^{c_2} \pmod{n}$.
   Déterminer une relation de Bezout $uc_1 + vc_2 = 1$ et calculer $C_1^u C_2^v \pmod{n}$.
2. Application numérique : $n = 143$, $c_1 = 7$, $c_2 = 17$, $C_1 \equiv 128 \pmod{n}$ et $C_2 \equiv 84 \pmod{n}$
   (a) Déterminer une relation de Bezout $uc_1 + vc_2 = 1$.
   (b) Calculer $C_1^u C_2^v \pmod{n}$.
   Indication : si $w < 0$ alors $C^w \equiv (C^{-1})^{|w|} \pmod{n}$.
   (c) En déduire $a \pmod{n}$.

Exercice 7

Cryptanalyse RSA utilisant le même exposant c et des modules RSA différents
Soit $j \geq 2$, $n_i : j$ modules RSA premiers entre eux deux à deux et $C_i : j$ messages chiffrés du même messsage clair a à l'aide du même entier c ($1 \leq i \leq j$).
On démontre que si $a^c < \prod_{i=1}^{j} n_i$ alors on peut déterminer le message clair a sans factoriser les modules.
Démonstration : le théorème des restes chinois permet de résoudre le système

$$\begin{cases} x \equiv C_1 \pmod{n_1} \\ x \equiv C_2 \pmod{n_2} \\ \quad \ldots \\ x \equiv C_j \pmod{n_j} \end{cases}$$

En posant $n = \prod_{i=1}^{j} n_i$, $\mathcal{S} = \{x_0 + kn,\ k \in \mathbb{Z}\} = \{x,\ x \equiv x_0 \pmod{n}\}$.

Si $a^c < n$ et si $x_0 < n$, alors $a^c = x_0$.
On peut alors calculer $a = \sqrt[c]{x_0}$.

On pose $n_1 = 205$, $n_2 = 253$, $n_3 = 493$ et $c = 3$.
On note C_1, C_2 et C_3 les messages chiffrés à partir du même message clair a avec les clés publiques (c, n_1), (c, n_2) et (c, n_3) : $C_1 \equiv a^c \pmod{n_1}$, $C_2 \equiv a^c \pmod{n_2}$ et $C_3 \equiv a^c \pmod{n_3}$.
On pose $C_1 \equiv 172 \,(\mathrm{mod}\, n_1)$, $C_1 \equiv 65 \,(\mathrm{mod}\, n_2)$ et $C_3 \equiv 134 \,(\mathrm{mod}\, n_3)$.
Et on suppose $a^c < n_1 n_2 n_3$.
On en déduit que a^c est la solution de

$$\begin{cases} x \equiv 172 \,(\mathrm{mod}\, n_1) \\ x \equiv 65 \,(\mathrm{mod}\, n_2) \\ x \equiv 134 \,(\mathrm{mod}\, n_3) \\ 0 \leq x < n_1 n_2 n_3 \end{cases}$$

1. Montrer
$$\begin{cases} x \equiv 172 \,(\mathrm{mod}\, n_1) \\ x \equiv 65 \,(\mathrm{mod}\, n_2) \end{cases} \Leftrightarrow x \equiv 27\,642 \,(\mathrm{mod}\, n_1 n_2).$$
2. Montrer
$$\begin{cases} x \equiv 27\,642 \,(\mathrm{mod}\, n_1 n_2) \\ x \equiv 134 \,(\mathrm{mod}\, n_3) \end{cases} \Leftrightarrow x \equiv 79\,507 \,(\mathrm{mod}\, n_1 n_2 n_3)$$
3. En déduire le message clair a.

Détail des calculs pour la résolution des deux systèmes

- $\begin{cases} x \equiv 172 \,(\mathrm{mod}\, n_1) \\ x \equiv 65 \,(\mathrm{mod}\, n_2) \end{cases}$
Relation de Bezout : : $PGCD(n_1, n_2) = 1$
$205 \times (-58) + 253 \times 47 = 1$
$x_{01} = 65 \times 205 \times (-58)) + 172 \times (253 \times 47) = 1\,272\,402$; $n_1 n_2 = 205 \times 253 = 51\,865$.
$1\,272\,402 \equiv 27\,642 \pmod{n_1 n_2}$; $1\,272\,402 \equiv 27\,642 \pmod{51\,865}$
$x'_{01} = 27\,642$
$\mathcal{S}_1 = \{27\,642 + 51\,865k,\ k \in \mathbb{Z}\} = \{x,\ x \equiv 27\,642 \,(\mathrm{mod}\, 51\,865)\}$
- $\begin{cases} x \equiv 27\,642 \,(\mathrm{mod}\, n_1 n_2) \\ x \equiv 134 \,(\mathrm{mod}\, n_3) \end{cases}$
Relation de Bezout : $PGCD(n_1 n_2, n_3) = 1$: $51\,865 \times 212 + 493 \times (-22\,303) = 1$
$x_{02} = 134 \times (212 \times 51\,865) + 27642 \times (493 \times (-22\,303)) = -302\,460\,885\,398$; $n_1 n_2 n_3 = 205 \times 253 \times 493 = 51\,865 \times 493 = 25\,569\,445$.
$-302\,460\,885\,398 \equiv 79\,507 \,(\mathrm{mod}\, 25\,569\,445)$
$0 \leq 79\,507 < n_1 n_2, n_3$: $x_0 = 79\,507$
$\mathcal{S} = \{79\,507 + 25\,569\,445k,\ k \in \mathbb{Z}\} = \{x,\ x \equiv 79\,507 \,(\mathrm{mod}\, 25\,569\,445)\}$

Cryptographie symétrique

Chiffrements par substitution mono-alphabétique

Exercice 8

Chiffrement de César ou par décalage
Le message chiffré se déduit du message en clair par un décalage des symboles de l'alphabet.
On note $\mathcal{A}$ un alphabet, $n = |\mathcal{A}|$ et k un entier positif appelé la clé.
Le message en clair est chiffré en additionnant au rang de chacun des symboles de l'alphabet le nombre k modulo n.
On appelle alors fonction de chiffrement la fonction $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie par $f(X) = X + K$ avec $K = \overline{k}$.
Remarques

- f est une permutation de $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire une bijection de $\mathbb{Z}/n\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.
- En posant $X = \overline{x}$, on peut aussi écrire $f(x) = x + k \pmod{n}$ pour simplifier les écritures.

Le déchiffrement se fait alors en utilisant la fonction de déchiffrement $f^{-1} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie par $f^{-1}(X) = X - K$, ou encore $f^{-1}(x) = x - k \pmod{n}$.
Exemple
$\mathcal{A} = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, *\}$ ($*$ représente l'espace), $n = |\mathcal{A}| = 27$ et $k = 10$.
On code chacun des symboles de l'alphabet en le remplaçant par son rang dans l'alphabet de la manière suivante.

Symbole	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Rang x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Symbole	O	P	Q	R	S	T	U	V	W	X	Y	Z	*	
Rang x	14	15	16	17	18	19	20	21	22	23	24	25	26	

Le message en clair *TOUR DE LA LIBERTE* est chiffré en additionnant au rang du symbole le nombre $k = 10$ modulo $n = 27$ ou $k = K$. La fonction de chiffrement $f : \mathbb{Z}/27\mathbb{Z} \to \mathbb{Z}/27\mathbb{Z}$ est définie par $f(X) = X + \overline{10}$ ou $f(x) = x + 10 \pmod{27}$.

Symbole	T	O	U	R	*	D	E	*	L	A	*	L	I	B	E	R	T	E
Rang x	19	14	20	17	26	3	4	26	11	0	26	11	8	1	4	17	19	4
Rang chiffré $x + 10 \pmod{27}$	2	24	3	0	9	13	14	9	21	10	9	21	18	11	14	0	2	14
Symbole chiffré	C	Y	D	A	J	N	O	J	V	K	J	V	S	L	O	A	C	O

On obtient donc le message chiffré *CYDAJNOJVKJVSLOACO*.
Le déchiffrement passe par la fonction de déchiffrement $f^{-1} : \mathbb{Z}/27\mathbb{Z} \to \mathbb{Z}/27\mathbb{Z}$ définie par $f^{-1}(X) = X - \overline{10}$ ou $f^{-1}(x) = x - 10 \pmod{27}$, ou encore $f^{-1}(x) = x + 17 \pmod{27}$. $k^{-1} = 17$ modulo $n = 27$ ou $k^{-1} = R$. Dans l'exemple, on obtient

Symbole chiffré	C	Y	D	A	J	N	O	J	V	K	J	V	S	L	O	A	C	O
Rang chiffré x	2	24	3	0	9	13	14	9	21	10	9	21	18	11	14	0	2	14
Rang déchiffré $x + 17 \pmod{27}$	19	14	20	17	26	3	4	26	11	0	26	11	8	1	4	17	19	4
Symbole déchiffré	T	O	U	R	*	D	E	*	L	A	*	L	I	B	E	R	T	E

Jules César utilisait la clé $k = 3$ dans sa correspondance avec ses proches.
Référence : Suétone (69-122).
Remarques

- On peut utiliser un symbole comme clé. Dans l'exemple, on aurait pu prendre la lettre K dont le rang est 10 dans l'alphabet. Le déchiffrement utilise alors la lettre de rang $-10 \equiv 17 \pmod{27}$, c'est-à-dire la lettre R.
- Il s'agit d'un exemple de chiffrement symétrique ou à clé secrète. La connaissance de la clé k facilite le calcul, tant de la fonction de chiffrement f, que la fonction de déchiffrement f^{-1}.
- Le chifrement de César utilise un ensemble de clés limité : il suffit d'essayer successivement toutes les clés possibles pour retrouver le message en clair à partir du message chiffré. Par ailleurs, on peut aussi s'intéresser à la fréquence des lettres de l'alphabet dans les textes pour retrouver la clé.

Fréquence des lettres de l'alphabet en français

E	A	S	I	N	T	R	L	U	O	D	C	M
17,35%	8,20%	7,93%	7,53%	7,17%	6,99%	6,65%	5,92%	5,73%	5,53%	4,01%	3,33%	2,97%

P	V	G	F	Q	H	B	X	J	Y	Z	K	W
2,92%	1,39%	1,09%	1,08%	1,04%	0,93%	0,92%	0,47%	0,34%	0,31%	0,11%	0,06%	0,03%

Source : Cryptographie et codes secrets - bibmath.net/crypto

Enoncé et questions
On reprend $\mathcal{A} = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, *\}$ ($*$ représente l'espace) avec $n = |\mathcal{A}| = 27$.

1. On note $k = 20$ ou encore $k = U$.
   (a) Ecrire la fonction f de chiffrement.
   (b) Chiffrer le message en clair *CRYPTOGRAPHIE*.
2. Un message a été chiffré par cette méthode et la même clé k. Le message chiffré obtenu est *YMTLYWNKBMY* (même alphabet).
   Préciser le message en clair et la clé de déchiffrement k'.

Exercice 9

Chiffrement affine
On note $\mathcal{A}$ un alphabet, $n = |\mathcal{A}|$ et la clé $k = (a, b) \in \mathbb{Z}^2$ avec $A = \overline{a}$ inversible dans $\mathbb{Z}/n\mathbb{Z}$.
La fonction de chiffrement s'écrit $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie par $f(X) = AX + B$ avec $B = \overline{b}$.
Remarques

- f est une permutation de $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire une bijection de $\mathbb{Z}/n\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.
- En posant $X = \overline{x}$, on peut aussi écrire $f(x) = ax + b \pmod{n}$ pour simplifier les écritures.

Exemple
On reprend l'alphabet $\mathcal{A}$ de l'exercice précédent et on note $a = 14$ et $b = 3$.
D'après l'exercice 1, $\overline{14}$ est inversible dans $\mathbb{Z}/27\mathbb{Z}$ et $\overline{14}^{-1} = \overline{2}$.
La clé est donc $k = (14, 3)$ et la fonction de chiffrement s'écrit $f(X) = \overline{14}X + \overline{3}$ ou encore $f(x) = 14x + 3 \pmod{27}$.
On reprend le message en clair *TOUR DE LA LIBERTE* et on obtient :

Symbole	T	O	U	R	*	D	E	*	L	A	*	L	I	B	E	R	T	E
Rang x	19	14	20	17	26	3	4	26	11	0	26	11	8	1	4	17	19	4
Rang chiffré $14x+3 \pmod{27}$	26	10	13	25	16	18	5	16	22	3	16	22	7	17	5	25	26	5
Symbole chiffré	*	K	N	Z	Q	S	F	Q	W	D	Q	W	H	R	F	Z	*	F

Le message chiffré est donc **KNLQSFQWDQWHRFUF*
Détail pour les deux premiers symboles :
Le rang de T est chiffré $f(19) = 14 \times 19 + 3 = 269 \equiv 26 \pmod{27}$ qui est codé $*$.
Le rang de O est chiffré $f(14) = 14 \times 14 + 3 = 199 \equiv 10 \pmod{27}$ qui est codé K.

La fonction de déchiffrement est obtenue en résolvant l'équation $\overline{14}X + \overline{3} = Y$.
On obtient par équivalence :
$\overline{14}X = Y - \overline{3}$
$\overline{14}^{-1} \times \overline{14}X = \overline{14}^{-1}\left(Y - \overline{3}\right)$
$\overline{1}X = \overline{2}\left(Y - \overline{3}\right)$
$X = \overline{2}Y - \overline{2} \times \overline{3}$
$X = \overline{2}Y - \overline{6}$
et enfin $f^{-1}(X) = \overline{2}X - \overline{6}$ ou encore $f^{-1}(x) = 2x - 6 \pmod{27}$.
On peut donc déchiffrer le message chiffré :

Symbole chiffré	*	K	N	L	Q	S	F	Q	W	D	Q	W	H	R	F	U	*	F
Rang chiffré x	26	10	13	25	16	18	5	16	22	3	16	22	7	17	5	25	26	5
Rang déchiffré $2x-6 \pmod{27}$	19	14	20	17	26	3	4	26	11	0	26	11	8	1	4	17	19	4
Symbole déchiffré	T	O	U	R	*	D	E	*	L	A	*	L	I	B	E	R	T	E

Détail pour les deux premiers symboles :
Le rang de $*$ est déchiffré $f^{-1}(26) = 2 \times 26 - 6 = 46 \equiv 19 \pmod{27}$ qui est codé T.
Le rang de K est déchiffré $f^{-1}(10) = 2 \times 10 - 6 = 14$ qui est codé O.

Enoncé et questions
On reprend $\mathcal{A} = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, *\}$ ($*$ représente l'espace) avec $n = |\mathcal{A}| = 27$.
Un message a été chiffré en utilisant un chiffrement affine de clé $k = (a, b)$ inconnue. Les deux lettres les plus fréquentes dans le message chiffré sont P et X dans cet ordre. On fait donc l'hypothèse que la lettre E est chiffrée P et la lettre A est chiffrée X.

1. Déterminer la clé $k = (a, b)$.
2. Déchiffrer le message *VKM*.

Chiffrements par substitution poly-alphabétique

Exercice 10

Chiffrement de Vigenère
On note $\mathcal{A}$ un alphabet, $n = |\mathcal{A}|$.
La clé k est une suite de m lettres écrites sous le message en clair. On additionne ensuite les deux textes modulo n.
Exemple
On reprend l'alphabet $\mathcal{A}$ de l'exercice précédent et on note la clé $k = ABCD$.

Symbole	T	O	U	R	*	D	E	*	L	A	*	L	I	B	E	R	T	E
Clé k	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D	A	B
Rang x	19	14	20	17	26	3	4	26	11	0	26	11	8	1	4	17	19	4
Rang clé x_k	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1
Rang chiffré $f(x) = x + x_k$	19	15	22	20	26	4	6	2	11	1	1	14	8	2	6	20	19	5
Symbole chiffré	T	P	W	U	*	E	G	C	L	B	B	O	I	C	G	U	T	F

On obtient donc le message chiffré : *TPWU*EGCLBBOICGUTF*.
Remarque : le chiffrement de César est un cas particulier de ce chiffrement qui le complique (augmentation du nombre de clés).
Référence : *Traité des chiffres ou secrètes manières d'écrire* de B. de Vigenère (1585).
Le déchiffrement s'opère de la manière suivante :

Symbole chiffré	T	P	W	U	*	E	G	C	L	B	B	O	I	C	G	U	T	F
Rang chiffré x	19	15	22	20	26	4	6	2	11	1	1	14	8	2	6	20	19	5
Rang clé $-x_k$	0	−1	−2	−3	0	−1	−2	−3	0	−1	−2	−3	0	−1	−2	−3	0	−1
Rang déchiffré $f^{-1}(x) = x - x_k$	19	14	20	17	26	3	4	26	11	0	26	11	8	1	4	17	19	4
Clé k'	A	*	Z	Y	A	*	Z	Y	A	*	Z	Y	A	*	Z	Y	A	*
Symbole déchiffré	T	O	U	R	*	D	E	*	L	A	*	L	I	B	E	R	T	E

Pour retrouver la clé de chiffrement à partir du message chiffré, on peut utiliser le test de Kasiski ou le test de Friedman qui permettent de retrouver la longueur de la clé, puis on peut à nouveau utiliser la fréquence des lettres.

Test de Kasiski
En 1863, Friedrich Kasiski a publié une méthode générale pour décoder les chiffres de Vigenère que Babbage connaissait certainement avant.
La méthode consiste à essayer de trouver la longueur de la clé en utilisant le fait que dans un texte en clair, il peut y avoir des répétitions de groupes de symboles. Deux occurences d'une répétition peuvent être séparées d'un multiple de la longueur L de la clé. Dans ce cas, les deux occurences sont chiffrées de la même façon.
On cherche donc les répétitions dans le texte chiffré, on détermine la distance les séparant. Cette distance peut être un multiple de la longueur de la clé (il peut y avoir des coïncidences).

Exemple de texte chiffré ($N = 416$ symboles)
NNOETJAXQMLHXHZRUGNCWJSPCNCSMQ NLW E DVWAFI VZLYNLAAOLPGWGJHPH
GDCJLWWOAYOMXARWTPWVL YDQGOB DPVWGNPLMNDEYXIFOUUEILZVIYSFXUY
CIHMRND SFNX FTPGLDYCMWIWYDXHGDMLMKZRFJEVVWMNIVJLOXIFOLYYXLMN
HEIVZDRWILOAYDUMDMIYRWICMZMPVWNPHASWYFJUJWMZRFZBWZRLMNWTRIP
JHEILMXCDZGTNF WIK JAWPWLVYYFTJZBMFMNVWNNILONJCSHJANTSFLDYDSFOO
ICQWNU YDQGOB XPW DVWAFI KHNLTHAJWU WIK OJHOMKLDY WIK DMCZQWNM
OYSJYBIYXAIOCYMEZWNAPMNAC NLW NNHN SFNX HYIKDUMLKAOMIYGVPWYWEF
BDYOYEDMC

Mot	Occurences	Positions	Distance	Décomposition	PGCD	Diviseurs
WIK	3	249, 327, 339	78, 12	$2 \times 3 \times 13$, $2^2 \times 3$	6	1,2,3,6
NLW	2	31, 375	344	$2^3 \times 43$	344	1,2,4,8,43,86,172,344
SFNX	2	124, 382	258	$2 \times 3 \times 43$	258	1,2,3,6,43,86,129,258
YDQGOB	2	80, 302	222	$2 \times 3 \times 37$	222	1,2,3,6,37,74,111,222
DVWAFI	2	35, 311	276	$2^2 \times 3 \times 23$	276	1,2,3,6,23,46,69,138,276

D'après ces résultats, une longueur de clé probable est un diviseur de 6 (1, 2, 3 ou 6).

Utilisation de l'indice de coïncidence : test de Friedman

On note $\mathcal{A}_0 = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\}$ et $n = |\mathcal{A}_0| = 26$.

L'indice de coïncidence IC d'un message est la probabilité que deux symboles pris au hasard dans un message de N symboles soient identiques (probabilité de répétition des symboles dans un message chiffré).

En notant n_i le nombre de symboles i dans l'alphabet, on obtient

$$IC = \sum_{i \in \mathcal{A}_0} \frac{n_i\,(n_i - 1)}{N\,(N-1)}$$

Démonstration

La probabilité que deux symboles pris au hasard soient un même symbole i donné est

$$\frac{C_{n_i}^2}{C_N^2} = \frac{\frac{n_i(n_i-1)}{2}}{\frac{N(N-1)}{2}} = \frac{n_i\,(n_i-1)}{N\,(N-1)}$$

- Dans un message dans lequel la fréquence de chacune des lettres est la même (message aléatoire : les symboles sont tirés uniformément de manière aléatoire) : $\frac{n_i}{N} = \frac{1}{n}$

  $$IC_a = \sum_{i \in \mathcal{A}} \frac{n_i\,(n_i-1)}{N\,(N-1)} = \sum_{i \in \mathcal{A}} \frac{N/n\,(N/n-1)}{N\,(N-1)} = n\frac{N/n\,(N/n-1)}{N\,(N-1)} = \frac{N-n}{n(N-1)}$$

  $$IC_a = N\frac{1-n/N}{nN(1-1/n)} = \frac{1-n/N}{n(1-1/N)} \approx \frac{1}{n} \text{ pour } N \text{ assez grand.}$$

  Pour $n = 26$, on obtient $IC_a = \frac{1}{26} \approx 0,03846$.

- Dans un langage structuré, l'indice de coïncidence ne dépend que de la distribution de probabilité des symboles et n'est pas modifié dans une substitution mono-alphabétique.

  En effet, pour tout tout entier k : $IC = \sum_{i+k \in \mathcal{A}_0} \frac{n_i\,(n_i-1)}{N\,(N-1)} = \sum_{i+k \in \mathcal{A}_0} \frac{n_i\,(n_i-1)}{N\,(N-1)}$ (avec $i + k$ modulo n).

  En prenant la table de la fréquence des lettres de l'alphabet en France, on obtient en posant $n_i - 1 \approx n_i$ et $N - 1 \approx N$:

  $$IC_F = \sum_{i \in \mathcal{A}_0} \frac{n_i\,(n_i-1)}{N\,(N-1)} = \sum_{i \in \mathcal{A}_0} \left(\frac{n_i}{N}\right)^2 \approx 0,07848.$$

  Remarque : en langue anglaise $IC_A \approx 0,0667$.

  Si l'indice de coïncidence d'un message chiffré est proche de IC_F alors le message a vraisemblablement été chiffré par une substitution mono-alphabétique.

  Remarque : si c'est le cas, on peut aussi avoir un renseignement sur la langue utilisée. Sinon, on suppose le chiffrement de Vigenère a été utilisé avec une clé de longueur $L \geq 2$, on détermine les L sous-messages M_i formés des symboles dont la position est respectivement congrue à $i = 1$, 2..., L modulo L. Dans chacun de ces groupes, les symboles ont été obtenus par un chiffrement de César qui ne modifie pas l'indice de coïncidence $IC_F \approx 0,07848$ du message en clair. On calcule alors l'indice de coïncidence des L sous-messages M_i et on en prend la moyenne. Si le résultat est proche de $IC_F \approx 0,07848$, on peut considérer avoir trouvé la longueur de la clé. Sinon, on passe à l'entier $L + 1$.

  Exemple

  $\boldsymbol{L = 2}$

  $\boldsymbol{M_1}$: NOTAQLXZUNWSCCMNWDWFVLNAOPWJPGCLWAOXRTWLDGBPW
  NLNEXFUELVYFUCHRDFXTGDCWWDHDLKRJVWNVLXFLYLNEVDWLAD
  MMYWCZPWPAWFUWZFBZLNTIJELXDGNWKAPLYFJBFNWNLNCHATFD

DFOCWUDGBPDWFKNTAWWKJOKDWKMZWMYJBYAOYEWAMANWNNF
XYKULAMYVWWFDOEM

$\boldsymbol{M_2}$: NEJXMHHRGCJPNSQLEVAIZYLALGGHHDJWOYMAWPVYQODVGPM
DYIOUIZISXYIMNSNFPLYMIYXGMMZFEVMIJOIOYXMHIZRIOYUDIRIMMV
NHSYJJMRZWRMWRPHIMCZTFIJWWVYTZMMVNIOJSJNSLYSOIQNYQOX
WVAIHLHJUIOHMLYIDCQNOSYIXICMZNPNCLNHSNHIDMKOIGPYEBYYDC

$\boldsymbol{L = 3}$

$\boldsymbol{M_1}$: NEAMXRNJCSNEWILLOGJHCWAMRPLQBVNMEIUIVSUIRSXPDMWXD
MREWILILXNIDIAUMRCMWHWJWRBRNRJIXZNIAWYTBMWINSASDSOQU
QBWWINHWIJMDIMQMSBXOMWPALNSXIUKMGWEDYM

$\boldsymbol{M_2}$: NTXLHUCSNMLDAVYALWHGJWYXWWYGDWPNYFULIFYHNFFGYW
YHMKFVMVOFYLHVRLYMIWMPNAYUMFWLWIHLCGFKWLYJMNNLJHNF
YFIWYGXDAKLAUKHKYKCWOJIACENMCWHFHKMAIVYFYEC

$\boldsymbol{M_3}$: OJQHZGWPCQWVFZNAPGPDLOOATVDOPGLDXOEZYXCMDNTLCID
GLZJVNJXOYMEZWODDYIZVPSFJZZZMTPEMDTWJPVFZFVNOCJTLDOCN
DOPVFHTJWOOLWDZNYYYIYZANNNNNYDLOYPWBOD

et ainsi de suite...

$\boldsymbol{L = 6}$

$\boldsymbol{M_1}$: NAXNCNWLOJCARLBNEUVURXDWDRWLLNDAMCWWWBNJXNAYB
WNADOUBWNWJDMMBOWANXUMWDM

$\boldsymbol{M_2}$: NXHCNLAYLHJYWYDPYUIYNFYYMFMOYHRYIMNYMWWHCFWYMN
JNYIYXALUHYCOICNCHHMIYYC

$\boldsymbol{M_3}$: OQZWCWFNPPLOTDPLXEYCDTCDLJNXYEWDYZPFZZTEDWPFFNCT
DCDPFTWOWZYYYANNYLYWO

$\boldsymbol{M_4}$: EMRJSEILGHWMPQVMIISISPMXMEIIXIIURMHJRRRIZIWTMISSSQQWI
HIMIQSXMPLSIKGEY

$\boldsymbol{M_5}$: TLUSMDVAWGWXWGWNFLFHFGWHKVVFLVLMWPAUFLILGKLJNL
HFFWGDKAKKKWJAEMWFKAVFE

$\boldsymbol{M_6}$: JHGPQVZAGDOAVOGDOZXMNLIGZVJOMZODIVSJZMPMTJVZVOJLO
NOVHJOLDNYIZNNNDOPBD

Longueur de la clé L	IC moyen
1	0,044775
2	0,052489
3	0,054857
4	0,051671
5	0,044459
6	0,075419

On en déduit que L vaut certainement 6, ce qui rejoint le résultat du test de Kasiski. Il reste alors à déterminer les 6 lettres associées aux 6 sous-messages M_1 à M_6. On peut alors y repérer les symboles les plus fréquents et les associer aux symboles les plus fréquents de la langue utilisée.

Enoncé et questions

On prend $\mathcal{A}_0 = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\}$ avec $n = |\mathcal{A}_0| = 26$.

On code chacune des symboles de l'alphabet en le remplaçant par son rang dans l'alphabet de la manière suivante.

Symbole	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang x	0	1	2	3	4	5	6	7	8	9	10	11	12
Symbole	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang x	13	14	15	16	17	18	19	20	21	22	23	24	25

Un message a été obtenu en appliquant le chiffrement de Vigenère sur un message en langue française dans lequel les espaces ont été supprimés.
L'indice de coïncidence moyen a été calculé à partir des sous-messages chiffrés en fonction de la longueur de la clé supposée :

Longueur de la clé L	IC moyen
1	0,0422381
2	0,050597
3	0,053110
4	0,049385
5	0,076257

1. Quelle est a priori la longueur L_k de la clé k ?
2. En supposant $L_k = 5$, le symbole le plus fréquent dans chacun des sous-messages M_i formés des symboles dont la position dans le message chiffré est respectivement congrue à $i = 1, 2..., L$ modulo L est

Sous-message	Symbole le plus fréquent
1	T
2	S
3	I
4	Q
5	I

Déchiffrer le début du message *JBEOVDGXUGWSIEX*.

Exercice 11

Chiffrement de Hill
On note $\mathcal{A}$ un alphabet, $n = |\mathcal{A}|$.
La clé est une matrice carrée inversible M d'ordre p dans $\mathbb{Z}/n\mathbb{Z}$. Le chiffrement opère sur des suites de p symboles.
Le message chiffré correspondant à un message clair $(X_1, X_2, ..., X_p) \in (\mathbb{Z}/n\mathbb{Z})^p$ est le vecteur $(Y_1, Y_2, ..., Y_p) \in (\mathbb{Z}/n\mathbb{Z})^p$ obtenu par la multiplication matricielle (algorithme ligne-colonne) :

$$f\begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_p \end{pmatrix} = M\begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_p \end{pmatrix} = \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_p \end{pmatrix}$$

Le déchiffrement s'effectue en multipliant le message chiffré par l'inverse M^{-1} de la matrice M.
M^{-1} est, lorsqu'elle existe, la matrice vérifiant $M \times M^{-1} = M^{-1} \times M = I_p$ où I_p est la matrice unité ou identité d'ordre p comportant des $\overline{1}$ sur la diagonale principale et des $\overline{0}$ ailleurs.
On s'intéresse ici au cas $p = 2$.
La matrice $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ à coefficients dans $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement
$det\ M = \begin{vmatrix} A & B \\ C & D \end{vmatrix} = AD - BC$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire $PGCD(\delta, n) = 1$ en

notant δ un représentant de $\Delta = det\ M$ modulo n.
On a alors $M^{-1} = (AD - BC)^{-1} \begin{pmatrix} D & -B \\ -C & A \end{pmatrix}$. Ici, $I_p = I_2 = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}$.

Exemple
On reprend l'alphabet $\mathcal{A}$ des exercices précédents, $|\mathcal{A}| = 27$.
En prenant $M = \begin{pmatrix} \overline{9} & \overline{2} \\ \overline{7} & \overline{6} \end{pmatrix}$ à coefficients dans $\mathbb{Z}/27\mathbb{Z}$, on obtient $det\ M = \overline{9} \times \overline{6} - \overline{7} \times \overline{2} = \overline{54} - \overline{14} = \overline{40} = \overline{13}$.
On a $PGCD(\delta, n) = PGCD(13, 27) = 1$ et M est donc inversible dans $\mathbb{Z}/27\mathbb{Z}$. La matrice inversible M est la clé de la méthode.
On découpe alors le message en clair en blocs de deux caractères : *TO UR *D E* LA *L IB ER TE* et on met en œuvre la multiplication.
TO est codé 19 14. On a alors
$\begin{pmatrix} \overline{9} & \overline{2} \\ \overline{7} & \overline{6} \end{pmatrix} \begin{pmatrix} \overline{19} \\ \overline{14} \end{pmatrix} = \begin{pmatrix} \overline{10} \\ \overline{1} \end{pmatrix}$ qui est décodé *KB*.

UR est codé 20 17. On a alors
$\begin{pmatrix} \overline{9} & \overline{2} \\ \overline{7} & \overline{6} \end{pmatrix} \begin{pmatrix} \overline{20} \\ \overline{17} \end{pmatrix} = \begin{pmatrix} \overline{25} \\ \overline{26} \end{pmatrix}$ qui est décodé *Z**.
On continue ainsi et on obtient alors : *KB Z* YL HW SX NF UI QW RW*, c'est-à-dire le message chiffré :
*KBZ*YLHWSXNFUIQWRW*.
Remarque : on peut regrouper les deux multiplications décrites en écrivant
$\begin{pmatrix} \overline{9} & \overline{2} \\ \overline{7} & \overline{6} \end{pmatrix} \begin{pmatrix} \overline{19} & \overline{20} \\ \overline{14} & \overline{17} \end{pmatrix} = \begin{pmatrix} \overline{10} & \overline{25} \\ \overline{1} & \overline{26} \end{pmatrix}$
Globalement, on peut calculer $M \times M_o = M_c$ (M_o : matrice du message en clair ou d'origine ; M_c : matrice du message chiffré) :
$\begin{pmatrix} \overline{9} & \overline{2} \\ \overline{7} & \overline{6} \end{pmatrix} \begin{pmatrix} \overline{19} & \overline{20} & \overline{26} & \overline{4} & \overline{11} & \overline{26} & \overline{8} & \overline{4} & \overline{19} \\ \overline{14} & \overline{17} & \overline{3} & \overline{26} & \overline{0} & \overline{11} & \overline{1} & \overline{17} & \overline{4} \end{pmatrix} = \begin{pmatrix} \overline{10} & \overline{25} & \overline{24} & \overline{7} & \overline{18} & \overline{13} & \overline{20} & \overline{16} & \overline{17} \\ \overline{1} & \overline{26} & \overline{11} & \overline{22} & \overline{23} & \overline{5} & \overline{8} & \overline{22} & \overline{22} \end{pmatrix}$
Le déchiffrement passe par l'utilisation de M^{-1}.
$M^{-1} = \overline{13}^{-1} \begin{pmatrix} \overline{6} & -\overline{2} \\ -\overline{7} & \overline{9} \end{pmatrix}$.
On obtient une relation de Bezout, par exemple grâce à l'algorithme d'Euclide : $27 \times 1 + 13 \times (-2) = 1$ qui conduit à $\overline{13} \times \overline{-2} = \overline{1}$ et donc à $\overline{13}^{-1} = -\overline{2} = \overline{25}$.
on a alors $M^{-1} = (-\overline{2}) \begin{pmatrix} \overline{6} & -\overline{2} \\ -\overline{7} & \overline{9} \end{pmatrix} = \begin{pmatrix} (-\overline{2}) \times \overline{6} & (-\overline{2}) \times (-\overline{2}) \\ (-\overline{2}) \times (-\overline{7}) & (-\overline{2}) \times \overline{9} \end{pmatrix} = \begin{pmatrix} \overline{15} & \overline{4} \\ \overline{14} & \overline{9} \end{pmatrix}$.
On déchiffre *KB* codé 10 1 :
$\begin{pmatrix} \overline{15} & \overline{4} \\ \overline{14} & \overline{9} \end{pmatrix} \begin{pmatrix} \overline{10} \\ \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{19} \\ \overline{14} \end{pmatrix}$
et on obtient 19 14 qui est décodé *TO*.
De même pour *Z** codé 25 26 :
$\begin{pmatrix} \overline{15} & \overline{4} \\ \overline{14} & \overline{9} \end{pmatrix} \begin{pmatrix} \overline{25} \\ \overline{26} \end{pmatrix} = \begin{pmatrix} \overline{15} & \overline{4} \\ \overline{14} & \overline{9} \end{pmatrix} \begin{pmatrix} -\overline{2} \\ -\overline{1} \end{pmatrix} = \begin{pmatrix} \overline{20} \\ \overline{17} \end{pmatrix}$
et on obtient 20 17 qui est décodé *UR*.
On peut aussi écrire
$\begin{pmatrix} \overline{15} & \overline{4} \\ \overline{14} & \overline{9} \end{pmatrix} \begin{pmatrix} \overline{10} & \overline{25} \\ \overline{1} & \overline{26} \end{pmatrix} = \begin{pmatrix} \overline{19} & \overline{20} \\ \overline{14} & \overline{17} \end{pmatrix}$.
Globalement, on peut calculer $M_d = M^{-1} \times M_c$ (M_d : matrice du message déchiffré ; M_c : matrice du message chiffré) :

$$\begin{pmatrix} \overline{15} & \overline{4} \\ \overline{14} & \overline{9} \end{pmatrix} \begin{pmatrix} \overline{10} & \overline{25} & \overline{24} & \overline{7} & \overline{18} & \overline{13} & \overline{20} & \overline{16} & \overline{17} \\ \overline{1} & \overline{26} & \overline{11} & \overline{22} & \overline{23} & \overline{5} & \overline{8} & \overline{22} & \overline{22} \end{pmatrix} = \begin{pmatrix} \overline{19} & \overline{20} & \overline{26} & \overline{4} & \overline{11} & \overline{26} & \overline{8} & \overline{4} & \overline{19} \\ \overline{14} & \overline{17} & \overline{3} & \overline{26} & \overline{0} & \overline{11} & \overline{1} & \overline{17} & \overline{4} \end{pmatrix}$$

On retrouve bien le message en clair *TO UR *D E* LA *L IB ER TE*, c'est-à-dire *TOUR DE LA LIBERTE*.

Remarques

- Dans le cas $p = 1$, on retrouve un chiffrement affine $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, définie par $f(X) = AX$, $A \in \mathbb{Z}/n\mathbb{Z}$.
- On peut remplacer chacune des classes par un représentant et faire les calculs modulo n.

Enoncé et questions

On prend $\mathcal{A}_0 = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\}$ avec $n = |\mathcal{A}_0| = 26$.

Un message a été obtenu en appliquant le chiffrement de Hill sur un message en langue française dans lequel les espaces ont été supprimés : *DVRD*.

La matrice à coefficients dans $\mathbb{Z}/26\mathbb{Z}$ utilisée pour le chiffrement est $M = \begin{pmatrix} \overline{5} & \overline{2} \\ \overline{7} & \overline{7} \end{pmatrix}$.

1. Vérifier que la matrice M est inversible dans $\mathbb{Z}/26\mathbb{Z}$.
2. Calculer M^{-1}.
3. En déduire le message déchiffré.

Exercice 12

On reprend l'alphabet $\mathcal{A} = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, *\}$.

On chiffre le message *LEST* en *DKFM* par le chiffrement de Hill ($p = 2$).

Déterminer la clé de chiffrement M, matrice à coefficients dans $\mathbb{Z}/27\mathbb{Z}$.

Indication

On peut résoudre l'équation d'inconnue $M \times M_o = M_c$ (M_o : matrice du message en clair ; M_c : matrice du message chiffré) avec $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ à coefficients dans $\mathbb{Z}/27\mathbb{Z}$.

Après avoir vérifié que M_o est inversible, on pourra alors montrer : $M = M_c \times M_o^{-1}$ et calculer M.

Formulaire

Relation

Relation binaire

Une relation binaire $\mathfrak{R}$ sur E est

1. réflexive
   si $\forall x\ x\mathfrak{R}x$
2. symétrique
   si $\forall x\ \forall y\ (x\mathfrak{R}y) \Rightarrow (y\mathfrak{R}x)$
3. antisymétrique
   si $\forall x\ \forall y\ (x\mathfrak{R}y) \wedge (y\mathfrak{R}x) \Rightarrow x = y$
4. transitive
   si $\forall x\ \forall y\ \forall z\ (x\mathfrak{R}y) \wedge (y\mathfrak{R}z) \Rightarrow x\mathfrak{R}z$

Relation d'équivalence

Une relation binaire sur E est une relation d'équivalence si elle est réflexive, symétrique et transitive.

Classes d'équivalence

Etant donnée une relation d'équivalence $\mathfrak{R}$ sur un ensemble E, on appelle classe d'équivalence modulo $\mathfrak{R}$: $\overline{x} = \{y \in E,\ y \equiv x\ (\mathrm{mod}\mathfrak{R})\}$.

Relation d'ordre

Une relation binaire sur E est une relation d'ordre si elle est réflexive, antisymétrique et transitive.

Ordre total, ordre partiel

On dit qu'une relation $x \preccurlyeq y$ est d'ordre total si, quels que soient les éléments x et y de E, on a $x \preccurlyeq y$ ou $y \preccurlyeq x$.

Dans le cas contraire, E est dit partiellement ordonné.

Treillis

Un ensemble ordonné $(E, \leq)$ est un treillis si pour tout $x \in E$ et tout $y \in E$ $x \vee y$ (plus petit majorant) et $x \wedge y$ (plus grand minorant) existent.

Treillis distributif

On dit qu'un treillis E est distributif, si pour tous x, y, z on a $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ et $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Complément

Soit E un treillis ayant un plus grand élément et un plus petit élément.

On dit qu'un élément x de E est complémenté s'il existe au moins un élément y de E tel que $x \vee y = sup(E)$ et $x \wedge y = inf(E)$.

Un tel élément y est dit complément de x.

Treillis complémenté

On dit qu'un treillis est complémenté si chacun de ses éléments possède au moins un complément.

Algèbre de Boole

Un treillis qui a au moins deux éléments et qui est distributif et complémenté est une algèbre de Boole.

Propriété

Dans une algèbre de Boole, chaque élément a un unique complément.

Notation

Le complément d'un élément x d'une algèbre de Boole est noté $\overline{x}$.

Relation

Application

Soient $f : E \to F$ une application.

1. f est injective si tout élément y de F admet au plus un antécédent par f.
2. f est surjective si tout élément y de F admet au moins un antécédent par f.
3. f est bijective si f est injective et surjective, c'est-à-dire si tout élément y de F admet exactement un antécédent par f.

Composition

Si $f : E \to F$ et $g : F \to G$.

L'application $h : E \to G$ définie par $h(x) = g(f(x))$ s'appelle l'application composée de g et de f.

Notation : $h = g \circ f$

On a donc : $\forall x \in E \; g \circ f(x) = g(f(x))$.

La composition des applications est associative.

Bijection

Si $f : E \to F$ est bijective alors $f^{-1} : F \to E$ définie par $y = f(x) \Leftrightarrow f^{-1}(y) = x$ est bijective.

$f^{-1} \circ f = id_E$

$f \circ f^{-1} = id_F$

Structures

Groupe

On dit que $G \neq \emptyset$ est un groupe pour la loi de composition interne $*$ s'il vérifie les axiomes :

1. associativité
   $\forall\ x,\ y,\ z \in E\ (x * y) * z = x * (y * z)$
2. $\exists e \in G\ \forall x \in G : x * e = e * x = x$
   e est appelé élément neutre
3. $\forall x \in G\ \exists x' \in G,\ x * x' = x' * x = e$
   x' est appelé symétrique

Le groupe est dit commutatif, ou abélien, s'il vérifie en plus : $\forall\ x,\ y \in G,\ x * y = y * x$.
L'élément neutre et le symétrique d'un élément sont uniques.

Anneau

Un anneau est un groupe commutatif A (noté additivement) sur lequel se trouve définie une deuxième loi de composition interne (notée multiplicativement) vérifiant les deux axiomes :

1. elle est associative et possède un élément neutre (appelé élément unité de l'anneau)
2. pour tout $x,\ y,\ z \in A$ on a : $(x+y)z = xz+yz$ et $z(x+y) = zx+zy$ (distributivité à droite et à gauche de la multiplication par rapport à l'addition).

Corps

Eléments inversibles

Un élément x de A est dit inversible s'il existe $x' \in A$ tel que $xx' = x'x = 1$.

Corps

Si un anneau A est tel que $1 \neq 0$ et tel que tout élément non nul soit inversible, on dit que c'est un corps.
Si la multiplication est commutative, on dit que le corps est commutatif.

Espace vectoriel

Soit $\mathbb{K}$ un corps commutatif.
Un $\mathbb{K}$ espace vectoriel E est un groupe commutatif (noté additivement) sur lequel est défini une loi scalaire :

$$\begin{array}{ccc} \mathbb{K} \times E & \to & E \\ (\lambda, x) & \mapsto & \lambda x \end{array}$$

vérifiant les axiomes suivants :

1. $\forall \lambda \in \mathbb{K},\ \forall x, y \in E\ \lambda(x+y) = \lambda x + \lambda y$
2. $\forall \lambda, \mu \in \mathbb{K},\ \forall x, y \in E\ (\lambda+\mu)x = \lambda x + \mu x$
3. $\forall \lambda, \mu \in \mathbb{K},\ \forall x \in E\ \lambda(\mu x) = (\lambda\mu)x$
4. $\forall x \in E\ 1x = x$ (1 élément unité de $\mathbb{K}$).

Cas particulier : $\mathbb{K} = \mathbb{R}$.

Arithmétique

Factorielle

$0! = 1$; $n! = n \times (n-1)!$ pour $n \geq 1$

$1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$

Arrangement

$A_n^p = \dfrac{n!}{(n-p)!}$

Combinaison

$C_n^p = \dfrac{n!}{(n-p)!p!}$

$C_n^0 = 1$

$C_n^1 = n$

$C_n^2 = \dfrac{n(n-1)}{2}$

$C_n^p = C_n^{n-p}$

$C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$ $(1 \leq p \leq n-1)$

Triangle de Pascal

$n\backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1
...							

Formule du binôme de Newton

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$$

$$= C_n^0 a^n b^0 + C_n^1 a^{n-1} b^1 + C_n^2 a^{n-2} b^2 + \cdots + C_n^{n-1} a^1 b^{n-1} + C_n^n a^0 b^n$$

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$$

$$(1+x)^n = \sum_{k=0}^{n} C_n^k x^k$$

$$= 1 + x + C_n^2 x^2 + C_n^3 x^3 + \cdots + C_n^n x^n$$

Autre formule : $a^n - b^n = (a-b) \sum_{k=1}^{n} a^{n-k} b^{k-1}$

$$= (a-b)\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + ... + a^2 b^{n-3} + ab^{n-2} + b^{n-1}\right)$$

Division euclidienne

Division euclidienne dans $\mathbb{N}$

Soient a et b deux entiers naturels $(b \neq 0)$.

Il existe un unique couple d'entiers naturels (q, r) tel que $a = bq + r$ et $0 \leq r < b$ (égalité de la division euclidienne).

q est apelé le quotient et r le reste.

Division euclidienne dans $\mathbb{Z}$

Soient a et b deux entiers relatifs $(b \neq 0)$.

Il existe un unique couple d'entiers relatifs (q,r) tel que $a = bq + r$ et $0 \leq r < |b|$.

Numération

Soit b un entier $(b > 2)$.

Tout entier naturel $a \neq 0$ s'écrit d'une manière unique sous la forme :

$a_p b^p + a_{p-1} b^{p-1} + a_{p-2} b^{p-2} + \cdots + a_2 b^2 + a_1 b^1 + a_0$

avec $0 \leq a_i < b$ $(0 \leq i \leq p)$ et $a_p \neq 0$ $(p \in \mathbb{N})$

PGCD

$a\mathbb{Z} + b\mathbb{Z} = PGCD(a,b)\mathbb{Z}$

PPCM

$a\mathbb{Z} \cap b\mathbb{Z} = PPCM(a,b)\mathbb{Z}$

Lemme d'Euclide

1. Si p est premier et $p|ab$ alors $p|a$ ou $p|b$
2. Si $a|bc$ et $PGCD(a,b) = 1$ alors $a|c$
3. Si $PGCD(a,b) = 1$, si $a|n$ et $b|n$ alors $ab|n$.

Théorème fondamental de l'arithmétique

La décomposition en facteurs premiers d'un entier est définie de manière unique (à l'ordre des facteurs près).

Petit théorème de Fermat

Si p est premier et a n'est pas un multiple de p alors $a^{p-1} \equiv 1 \pmod{p}$.

Corollaire

Si p est premier alors pour tout entier a

$a^p \equiv a \pmod{p}$.

Théorème du reste chinois

Soient a et b deux entiers quelconques.

Si m et n sont premiers entre eux ($m \geq 2$, $m \geq 2$) alors $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ a pour solution $S = \{x_0 + kmn,\ k \in \mathbb{Z}\}$ avec x_0 solution particulière du système.

Remarques

1. $S = \{x \in \mathbb{Z},\ x \equiv b \pmod{n}\}$
2. En notant $mu + nv = 1$ (décomposition de Bezout), on peut prendre $x_0 = mub + nva$.

Nombres premiers

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541