ircam Centre Pompidou

UPMC SORBONNE UNIVERSITÉS

Bases de l'Arithmétique & Cryptologie Romantique

Ninon Devis: ninon.devis@ircam.fr

TD3

Exercice 9 – Indice de coïncidence mutuelle

1. Sachant que le texte suivant a été chiffré en utilisant une clé de taille 4 et le cryptosystème de Vigenère, retrouvez le texte clair en utilisant la table des indices de coïncidence mutuelle suivante.

- Rappels: Indice de coïncidence mutuelle: distingue l'aléatoire sur deux textes.
  - Attaque sur la clef.
- L'ICM entre deux textes t_1 et t_2 est la probabilité de tirer au hasard la même lettre dans t_1 et t_2

$$ICM = \sum_{i=0}^{25} \frac{m_i n_i}{m n}$$

avec: m_i: nombre de caractères c_i dans t_1 — m: taille de t_1

n_i: nombre de caractères c_i dans t_2 — n: taille de t_2

Exercice 9 – Indice de coïncidence mutuelle

0	1	2	3
W	W	W	J
J	R	K	Y
T	B	X	F
D	Z	H	T
…	…	…	…

- Explication sur la construction tableau:
  - Le texte est d'abord découpé en 4 colonnes (taille de la clef):
  - On calcule ensuite l'ICM entre une colonne i (référence de l'aléatoire) et une colonne j à laquelle on applique les 25 permutations de l'alphabet.

➔ A la bonne permutation sur j: IMC élevé!

  - On a trouvé le bon décalage entre la colonne i et j pour avoir un texte qui n'est pas aléatoire.

"ICM entre s_i et Dec(s_j, d)"
=
"ICM entre la colonne i et décalage de la colonne j pour la lettre d"

i	j	Indice de coïncidence mutuelle entre s_i et $\mathrm{Dec}(s_j, d)$ avec $d = 0, \ldots, 25$												
0	1	0.034	0.064	0.038	0.042	0.027	0.041	0.040	0.031	0.031	0.034	0.039	0.029	0.045
		0.028	0.041	0.033	0.047	0.035	0.037	0.034	0.044	0.046	0.032	0.052	0.031	0.031
0	2	0.053	0.043	0.044	0.025	0.035	0.050	0.042	0.035	0.027	0.033	0.044	0.063	0.041
		0.033	0.027	0.042	0.037	0.033	0.033	0.035	0.036	0.029	0.040	0.032	0.043	0.034
0	3	0.024	0.029	0.039	0.063	0.045	0.028	0.026	0.047	0.034	0.035	0.036	0.038	0.032
		0.029	0.045	0.043	0.041	0.034	0.047	0.040	0.031	0.029	0.037	0.054	0.042	0.037
1	2	0.036	0.034	0.028	0.040	0.041	0.041	0.034	0.038	0.044	0.040	0.063	0.043	0.032
		0.030	0.044	0.039	0.034	0.038	0.035	0.027	0.027	0.042	0.039	0.037	0.033	0.049
1	3	0.036	0.040	0.065	0.042	0.024	0.029	0.046	0.037	0.029	0.046	0.040	0.021	0.033
		0.050	0.046	0.031	0.033	0.049	0.031	0.030	0.037	0.048	0.038	0.034	0.040	0.030
2	3	0.023	0.024	0.043	0.044	0.050	0.039	0.043	0.040	0.025	0.034	0.027	0.045	0.035
		0.045	0.041	0.023	0.034	0.043	0.076	0.040	0.025	0.031	0.032	0.045	0.034	0.048

Exercice 9 – Indice de coïncidence mutuelle

- Exemple pour i = 0 et j = 1

Si on permute une fois la colonne j, on obtient un IMC élevé.
(Rappel: IMC invariant par chiffrement par substitution.)

i	j	Indice de coïncidence mutuelle entre s_i et Dec(s_j, d) avec $d = 0, \ldots, 25$												
0	1	0.034	0.064	0.038	0.042	0.027	0.041	0.040	0.031	0.031	0.034	0.039	0.029	0.045
		0.028	0.041	0.033	0.047	0.035	0.037	0.034	0.044	0.046	0.032	0.052	0.031	0.031
0	2	0.053	0.043	0.044	0.025	0.035	0.050	0.042	0.035	0.027	0.033	0.044	0.063	0.041
		0.033	0.027	0.042	0.037	0.033	0.033	0.035	0.036	0.029	0.040	0.032	0.043	0.034
0	3	0.024	0.029	0.039	0.063	0.045	0.028	0.026	0.047	0.034	0.035	0.036	0.038	0.032
		0.029	0.045	0.043	0.041	0.034	0.047	0.040	0.031	0.029	0.037	0.054	0.042	0.037
1	2	0.036	0.034	0.028	0.040	0.041	0.041	0.034	0.038	0.044	0.040	0.063	0.043	0.032
		0.030	0.044	0.039	0.034	0.038	0.035	0.027	0.027	0.042	0.039	0.037	0.033	0.049
1	3	0.036	0.040	0.065	0.042	0.024	0.029	0.046	0.037	0.029	0.046	0.040	0.021	0.033
		0.050	0.046	0.031	0.033	0.049	0.031	0.030	0.037	0.048	0.038	0.034	0.040	0.030
2	3	0.023	0.024	0.043	0.044	0.050	0.039	0.043	0.040	0.025	0.034	0.027	0.045	0.035
		0.045	0.041	0.023	0.034	0.043	0.076	0.040	0.025	0.031	0.032	0.045	0.034	0.048

(1) (2) (3) (4) (5) (6)

- Combien de permutation sur la 3ème colonne doit-on effectuer pour ne plus avoir un texte aléatoire? 3 permutations.
- On peut résumer cela en systèmes:

(1) $d_0 - d_1 = 1$

(2) $d_0 - d_2 = 11$

(3) $d_0 - d_3 = 3$

(4) $d_1 - d_2 = 10$

(5) $d_1 - d_3 = 2$

(6) $d_2 - d_3 = 18$

Exercice 9 – Indice de coïncidence mutuelle

$$
\begin{aligned}
d_0 - d_1 &= 1 \\
d_0 - d_2 &= 11 \\
d_0 - d_3 &= 3 \\
d_1 - d_2 &= 10 \\
d_1 - d_3 &= 2 \\
d_2 - d_3 &= 18
\end{aligned}
$$

- Des trois premières équations, on déduit:

$d_1 = d_0 - 1$ $\quad$ $d_2 = d_0 - 11$ $\quad$ $d_3 = d_0 - 3$

- On injecte ces résultats dans les trois suivantes:

$d_1 - d_2 = (d_0 - d_2) - (d_0 - d_1) = 10$

$d_1 - d_3 = (d_0 - d_3) - (d_0 - d_1) = 2$

$d_2 - d_3 = (d_0 - d_3) - (d_0 - d_2) = -8 = 18 \mod 26$

➔ Le système est cohérent.

- Il reste à trouver la valeur de d_0: on calcule dans la colonne 0 la lettre la plus fréquente, il y a des chances alors qu'il s'agisse de E.
- On en déduit ensuite la valeur du décalage d_0, puis d_1, d_2, d_3 et donc la clef.

➔ Dans le texte il y a deux lettres les plus fréquentes: le C et le T. (10 fois chacunes)

Exercice 9 – Indice de coïncidence mutuelle

Rappels:
$d_1 = d_0 - 1$
$d_2 = d_0 - 11$
$d_3 = d_0 - 3$

➔ Si C est le chiffré de E dans la colonne 0:
- alors d_0 = C - E = -2 = 24 mod 26
- d'où: d_1 = 23 d_2 = 13 d_3 = 21
- La clef est donc: YXNV

➔ Si T est le chiffré de E dans la colonne 0:
- alors d_0 = T - E = 15
- d'où: d_1 = 14 d_2 = 4 d_3 = 12
- La clef est donc: POEM

Exercice 9 – Indice de coïncidence mutuelle

➔ Si la clef est YXNV:

```
YZJALUXDVEKKFCUYZDKYRKCFEXIFDREKZTGFVDJUVGVEUDFIVLGFEZETZUVEKKYREZEJGZ
IRKZFEREUKYRKKFLKKVIKYVGFVKIPFWIFDRETVCPIZTJNFLCUJLWWZTVYVETVYZJKYVFIP
TCVRICPWZKKVUKFYZJFNECZDZKRKZFEJKYRKRCFEXGFVDZJRWCRKTFEKIRUZTKZFEZEKVI
DJKYVTFDGFEVEKJFWKYVIRMVERIVWVNREUJZDGCVRDRERSZIUREUKYVGYREKRJDRCDVDFI
PRKRNFDRE
```

➔ Si la clef est POEM:

```
HISJUDGMENTTOLDHIMTHATLONGROMANTICPOEMSDEPENDMOREUPONINCIDENTTHANINSPI
RATIONANDTHATTOUTTERTHEPOETRYOFROMANCELYRICSWOULDSUFFICEHENCEHISTHEORY
CLEARLYFITTEDTOHISOWNLIMITATIONSTHATALONGPOEMISAFLATCONTRADICTIONINTER
MSTHECOMPONENTSOFTHERAVENAREFEWANDSIMPLEAMANABIRDANDTHEPHANTASMALMEMOR
YATAWOMAN
```

Exercice 11 – Inversion modulaire

1. Rappeler la définition de l'anneau A = Z/7Z.

- Définition d'un anneau: A est un anneau ⇔ A est un ensemble muni de deux lois de compositions internes notées + et x, tels que:
  - (A, +) est un groupe abélien dont le neutre sera noté 0_A
  - La loi x est associative: $\forall a, b, c \in A,\ a \times (b \times c) = (a \times b) \times c$
  - La loi x possède un élément neutre noté 1_A
  - La loi x est distributive à gauche et à droite par rapport à la loi +: $\forall a, b, c \in A,\ a \times (b + c) = a \times b + a \times c$
- Lorsque la loi x est commutative, on dit que l'anneau est commutatif.

➔ Z/7Z est l'ensemble des restes possibles de la division euclidienne par 7.

Exercice 11 – Inversion modulaire

1. Donner la table d'addition et de multiplication de A. L'anneau A possède-t-il des diviseurs de zéro ? Est-il intègre ? Est-il un corps ?

- Définition: Un anneau commutatif unitaire (A, +, x) est intègre s'il est:
  - différent de l'anneau nul
  - sans diviseur de zéro: $\forall a, b \in A^2 : a \times b = 0 \Rightarrow a = 0$ ou $b = 0$

→ Il n'y a aucun $a \times b = 0$ donc A est un anneau intègre

- Définition: Un corps est un ensemble muni de 2 opérations rendant possible l'addition, la soustraction, la multiplication et le calcul d'opposés et d'inverses. Tous les éléments sont inversibles

→ A est un corps.

inverses :

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

opposés :

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Exercice 11 – Inversion modulaire

1. Quelle est la différence majeure entre Z/7Z et Z/26Z ?

- Z/26Z est il un anneau intègre ? Est-il un corps ?

→ $\mathbb{Z}/26\mathbb{Z}$ a des diviseurs de 0 puisque : $2 \times 13 = 0$ et $2 \neq 0$ et $13 \neq 0$

→ $\mathbb{Z}/26\mathbb{Z}$ n'est pas un anneau intègre donc pas un corps.

2. Donner la définition d'un cryptosystème par chiffrement affine avec P = C = A. Quelle est la différence principale avec le cas où P = C = Z/26Z ?

- *Rappels*: P et C sont les alphabets pour écrire les messages clairs et chiffrés respectivement. K l'ensemble des clefs possibles. Pour tout $K \in \mathrm{K}$ on peut définir deux applications $e_K : \mathrm{P} \to \mathrm{C}$ (Encryption) et $d_K : \mathrm{C} \to \mathrm{P}$ (Decryption) telles que $d_K(e_K(x)) = x$ pour tout $x \in \mathrm{P}$.

- P = C = A, $\forall (a,b) \in \mathrm{K}$, $e_K(x) = ax + b \bmod 7$ et $d_K(x) = a^{-1}(y - b) \bmod 7$

Exercice 11 – Inversion modulaire

3. (**Chiffrement de Hill**) Le cryptosystème poly-alphabétique de Hill que nous allons étudier ici permet de chiffrer des données de deux caractères de l'alphabet Z/7Z. Une clé K sera représentée par une matrice 2 × 2 à coefficients dans Z/7Z et la fonction de chiffrement correspondante sera l'application de K sur un vecteur de deux caractères. Donner la représentation formelle de ce cryptosystème comme nous l'avons vu en cours. Quelle caractéristique doit avoir la matrice K pour que le cryptosystème soit valide ?

- Rappel: Chiffrement de Hill ?
  $P = C = A \times A$ et $K \subseteq M_2(A)$: à v, on associe $e_K(v) = Kv$
  ➔ le produit du vecteur v par la matrice K.

Pour pouvoir calculer $v = d_k(e_K(v))$ à partir de $e_K(v)$, il faut que la matrice K soit inversible.

Exercice 11 – Inversion modulaire

3. **Chiffrement de Hill**

- Les lettres sont remplacées par leur rang dans l'alphabet, les lettres P_k et P_{k+1} du texte clair seront chiffrées C_k et C_{k+1} selon la formule:

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} (mod 26)$$

- Le chiffrement obtenu est donc:
  - $C_k = a P_k + b P_{k+1}$
  - $C_{k+1} = c P_k + d P_{k+1}$
- Exemple: soit la clef $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$, on veut chiffrer 'je': J : 10, E : 5

$C_1 = 9 \times 10 + 4 \times 5 \ (mod 26) = 6$

$C_2 = 5 \times 10 + 7 \times 5 \ (mod 26) = 7$

J devient F

E devient G

Exercice 11 – Inversion modulaire

3. **Déchiffrement de Hill**

- Selon le même principe on prend les lettres 2 à 2, avec la formule:

$$\begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} (mod 26)$$

- Avec $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Rappel :

$A^{-1} = \frac{1}{\det A} {}^t\mathrm{com}\, A$

- Quelle propriété doit-on avoir sur K pour que K soit inversible ? $\det(K) \neq 0$!

Exercice 11 – Inversion modulaire

3. Le cryptosystème poly-alphabétique de Hill que nous allons étudier ici permet de chiffrer des données de deux caractères de l'alphabet Z/7Z. Une clé K sera représentée par une matrice 2 × 2 à coefficients dans Z/7Z et la fonction de chiffrement correspondante sera l'application de K sur un vecteur de deux caractères. Donner la représentation formelle de ce cryptosystème comme nous l'avons vu en cours. Quelle caractéristique doit avoir la matrice K pour que le cryptosystème soit valide ?

➔ $P = C = A$ et $K \subseteq M_2(A)$: à v, on associe: $\varepsilon_K(v) = Kv$

Pour pouvoir calculer: $v = d_K(\varepsilon_K(v))$

il faut que: K soit inversible.

Exercice 11 – Inversion modulaire

4. Montrer que l'ensemble des matrices 2 × 2 sur un anneau A forme lui-même un anneau et que le sous-ensemble des matrices inversibles est un groupe pour la multiplication.

a. Un anneau est un ensemble doté de deux lois de composition interne, l'une additive notée + et l'autre multiplicative notée ×.
b. L'addition est commutative, associative, admet un élément neutre et tout élément de l'anneau admet un opposé pour l'addition.
c. La multiplication est associative, distributive par rapport à l'addition et admet un élément neutre.

➔ a. Soient X, Y, Z $\in \mathrm{M}_2(\mathrm{A})$ tels que $X = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} Y = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} Z = \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}$

X + Y = $\begin{pmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{pmatrix}$ et X × Y = $\begin{pmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{pmatrix}$

➔ $\mathrm{M}_2(\mathrm{A})$ est stable par addition et multiplication de matrices.

Exercice 11 – Inversion modulaire

4. b. L'addition est commutative, associative, admet un élément neutre et tout élément de l'anneau admet un opposé pour l'addition.

➔ $X + Y = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix} = \begin{pmatrix} a_2 + a_1 & b_2 + b_1 \\ c_2 + c_1 & d_2 + d_1 \end{pmatrix} = Y + X$

➔ De la même manière: $(X + Y) + Z = X + (Y + Z)$

➔ Élément neutre pour l'addition: $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

➔ Quelle que soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ alors la matrice $-M = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ est son opposé.

Exercice 11 – Inversion modulaire

4. c. La multiplication est associative, distributive par rapport à l'addition et admet un élément neutre.

➔ Associativité: Il suffit de calculer $(X*Y)*Z$ et $X*(Y*Z)$: on retrouve le même résultat!

➔ Distributivité: Il suffit de calculer: $X*(Y+Z)$ et $X*Y+X*Z$: on retrouve le même résultat aussi.

➔ Élément neutre pour la multiplication: $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

➔ $M_2(A)$ est un anneau !

➔ Le sous-ensemble des matrices inversibles est un groupe pour la multiplication car chaque élément possède un inverse !

Exercice 11 – Inversion modulaire

5. Montrer que, lorsqu'elle existe, l'inverse d'une matrice A peut être calculée par la matrice complémentaire: $B = A^{-1} = \frac{1}{detA}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ ^M1

- Remarque: si l'anneau A est intègre alors l'anneau $M_2(A)$ l'est aussi car $\det AB = \det A \det B$ et A inversible est équivalent à $\det A \neq 0$

Mais ici on travaille dans A = Z/26Z qui n'est pas intègre.

➔ On calcule le produit AB: $AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \frac{1}{\det A} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$= \frac{1}{\det A} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{\det A} \times \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \frac{1}{\det A} \times \begin{pmatrix} \det A & 0 \\ 0 & \det A \end{pmatrix}$

$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$

Exercice 11 – Inversion modulaire

➔ On calcule le produit BA: $BA = \frac{1}{\det A}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$= \frac{1}{\det A} \times \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$

➔ Donc si det(A) = ab -bc ≠ 0, alors A est inversible et $B = A^{-1}$

➔ Si det(A) = 0, alors A n'est pas inversible

Exercice 11 – Inversion modulaire

6. Déduire de la question précédente un moyen de reconnaître une matrice inversible. Donner alors une nouvelle spécification du chiffrement de Hill, exhiber un exemple de chiffrement et déchiffrement pour une clé bien choisie.

➔ On vient de voir que A est inversible ⇔ $\det A \neq 0$

➔ Pour le chiffrement de Hill: On chiffre successivement des blocs de 2 caractères selon une matrice inversible modulo 7 de taille 2×2 en multipliant chaque bloc de 2 caractères par cette matrice.

➔ Exemple: soit la matrice $A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ avec $\det(A) = 2 \times 2 - 1 \times 3 = 1 \neq 0$

A est inversible modulo 7.

On chiffre le mot '123456': on le découpe en blocs représentés par des vecteurs:

$v_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, v_2 = \begin{pmatrix} 3 \\ 4 \end{pmatrix}, v_3 = \begin{pmatrix} 5 \\ 6 \end{pmatrix}$ et on multiplie chacun des vecteurs par A:

$v_1 \times A = \begin{pmatrix} 1 \\ 5 \end{pmatrix} \bmod 7 \qquad v_2 \times A = \begin{pmatrix} 4 \\ 4 \end{pmatrix} \bmod 7 \qquad v_3 \times A = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \bmod 7$

Donc le chiffré de '123456' est 154403