UNIVERSITÉ LAVAL

# Chapitre II : exercices + solutions

MOHAMED MEJRI

*Groupe LSFM*

*Département d'Informatique et de Génie Logiciel*

*Université LAVAL*

*Québec, Canada*

# Cryptanayse du chiffrement de Hill

- Question : Trouver la clé $K$ qui permet de transformer le message $CRYPTO$ en $VKLCAV$ en utilisant le chiffrement de Hill.
- Réponse :
  - 1er essai :

$$\begin{pmatrix} 2(C) & 17(R) \\ 24(Y) & 15(P) \end{pmatrix} K = \begin{pmatrix} 21(V) & 10(K) \\ 11(L) & 2(C) \end{pmatrix}$$

Si la matrice $\begin{pmatrix} 2(C) & 17(R) \\ 24(Y) & 15(P) \end{pmatrix}$ est inversible dans $\mathbb{Z}_{26}$ alors la valeur de $K$ sera :

$$K = \begin{pmatrix} 2(C) & 17(R) \\ 24(Y) & 15(P) \end{pmatrix}^{-1} \times \begin{pmatrix} 21(V) & 10(K) \\ 11(L) & 2(C) \end{pmatrix}$$

Puisque $det(\begin{pmatrix} 2(C) & 17(R) \\ 24(Y) & 15(P)) \end{pmatrix} = -378 \equiv 12 \ mod \ 26$ et $pgcd(12, 26) \neq 1$ donc la matrice $\begin{pmatrix} 2(C) & 17(R) \\ 24(Y) & 15(P) \end{pmatrix}$ n'est pas inversible dans $\mathbb{Z}_{26}$

# Cryptanayse du chiffrement de Hill

- Réponse (suite) :
  - 2me essai :

$$\begin{pmatrix} 2(C) & 17(R) \\ 19(T) & 14(O) \end{pmatrix} K = \begin{pmatrix} 21(V) & 10(K) \\ 0(A) & 21(V) \end{pmatrix}$$

Si la matrice $\begin{pmatrix} 2(C) & 17(R) \\ 19(T) & 14(O) \end{pmatrix}$ est inversible dans $\mathbb{Z}_{26}$ alors la valeur de $K$ sera :

$$K = \begin{pmatrix} 2(C) & 17(R) \\ 19(T) & 14(O) \end{pmatrix}^{-1} \times \begin{pmatrix} 21(V) & 10(K) \\ 0(A) & 21(V) \end{pmatrix}$$

Puisque $det(\begin{pmatrix} 2(C) & 17(R) \\ 19(T) & 14(O) \end{pmatrix}) = -295 \equiv 17 \ mod \ 26$ et $pgcd(17, 26) = 1$ donc la matrice $\begin{pmatrix} 2(C) & 17(R) \\ 19(T) & 14(O) \end{pmatrix}$ est inversible dans $\mathbb{Z}_{26}$ et son inverse est $\begin{pmatrix} 10 & 25 \\ 5 & 20 \end{pmatrix}$

On déduit que $K = \begin{pmatrix} 10 & 25 \\ 5 & 20 \end{pmatrix} \times \begin{pmatrix} 21 & 10 \\ 0 & 21 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$

# Cryptanayse du chiffrement affine

- Questions : Soit $m$ un message en français tel que :

$$e_k(m) = MRLAD\ UUERP\ RSKFU\ UDSRU\ FDKYF\ EKDOR\ MFLEZ$$
$$YKVXE\ FYADR\ LMFHH\ DBNRP\ VSVFM\ YAFIR\ KDBNR$$

  - Le système cryptograpphique utilisé pour crypter $m$ peut être le chiffrement de Vigenere ou un chiffrement affine. Trouver ce système sachant que $Ic(m) \approx 0.0575$.
  - Trouver le message $m$.
- Réponses :
  - Calcul d'indice de coïncidence de $e_k(m)$ :

| | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $n_i$ | 3 | 2 | 0 | 7 | 4 | 8 | 0 | 2 | 1 | 0 | 5 | 3 | 4 |
| $n_i * (n_i - 1)$ | 6 | 2 | 0 | 42 | 12 | 56 | 0 | 2 | 0 | 0 | 20 | 6 | 12 |

| | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $n_i$ | 2 | 1 | 2 | 0 | 9 | 3 | 0 | 5 | 3 | 0 | 1 | 4 | 1 |
| $n_i(n_i - 1)$ | 2 | 0 | 2 | 0 | 72 | 6 | 0 | 20 | 6 | 0 | 0 | 12 | 0 |

$$Ic(e_k(m)) = \frac{\sum_{i=0}^{25} n_i*(n_i-1)}{n*(n-1)} \approx 0.0575$$

Un système de chiffrement affine ne modifie pas l'indice de coïncidence. Puisque $Ic(e_k(m)) \approx Ic(m) \approx 0.0575$, on déduit qu'il y a une forte chance que le système cryptographique utilisé pour crypter $m$ soit un chiffrement affine.

  - Les lettres les plus fréquentes dans $e_k(m)$ sont $r > f > d < k = u > \ldots$. Les lettres les plus fréquentes dans la langue française sont $e > a > i > \ldots$.

# Cryptanayse du chiffrement affine

- Réponses (suite) :

$$\begin{cases} e_k(E) = R \\ e_k(A) = F \end{cases} \Leftrightarrow \begin{cases} e_k(4) = 17 \\ e_k(0) = 5 \end{cases} \Leftrightarrow \begin{cases} (4a+b)\ mod\ 26 = 17 \\ (b)\ mod\ 26 = 5 \end{cases} \Leftrightarrow \begin{cases} 4a\ mod\ 26 = 12 \\ (b)\ mod\ 26 = 5 \end{cases}$$

Remarque : puis que $4a\ mod\ 26 = 12$ et 4 n'est pas inversible dans $\mathbb{Z}_{26}$, donc zéro ou plusieurs valeurs de $a$ peuvent satisfaire l'équation. Dans notre cas, l'équation a deux solutions $a = 3$ et $a = 16$. D'autre équations comme $(2a\ mod\ 26 = 3)$ ne donnent pas de solutions.

$$\begin{cases} a = 3 \\ b = 5 \end{cases}$$

$pgcd(a, 26) = 1 \Rightarrow$ la solution est réalisable.

On conclu que $m =$ "Le chiffrement affine fait parti de la cryptographie classique monoalphabetique"

# Cryptanayse du chiffrement de Veginere

- Question : Décrypter le message suivant

KCCPK BGUFD PHQTY AVINR RTMVG RKDNB VFDET DGILT XRGUD DKOTF MBPVG EGLTG CKQRA CQCWD NAWCR XIZAK FTLEW
RPTYC QKYVX CHKFT PONCQ QRHJV AJUWE TMCMS PKQDY HJVDA HCTRL SVSKC GCZQQ DZXGS FRLSW CWSJT BHAFS IASPR
JAHKJ RJUMV GKMIT ZHFPD ISPZL VLGWT FPLKK EBDPG CEBSH CTJRW XBAFS PEZQN RWXCV YCGAO NWDDK ACKAW BBIKF
TIOVK CGGHJ VLNHI FFSQE SVYCL ACNVR WBBIR EPBBV FEXOS CDYGZ WPFDT KFQIY CWHJV LNHIQ IBTKH JVNPI ST

Sachant que le message original été encrypté avec un chiffrement de Vigenre en utilisant une clé de taille 6. Par ailleurs, les lettres les plus fréquentes dans $Y^0$ sont "q> g=j> v> c", et les $IC(Y^0, Y^i - k)$ $(1 \leq i \leq 5, 0 \leq k \leq 25)$ sont donnés par le tableau suivant :

| i | $IC(Y^0, Y^i - k), 0 \leq k \leq 25$ | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | .0393 | .0452 | .0430 | .0366 | .0421 | .0341 | .0277 | .0243 | .0507 | .0384 | .0372 | .0350 | .0473 |
| | .0326 | .0344 | .0747 | .0246 | .0320 | .0323 | .0307 | .0360 | .0477 | .0464 | .0332 | .0369 | .0363 |
| 2 | .0332 | .0369 | .0430 | .0440 | .0273 | .0375 | .0320 | .0384 | .0409 | .0473 | .0381 | .0409 | .0329 |
| | .0338 | .0289 | .0440 | .0477 | .0280 | .0381 | .0344 | .0372 | .0458 | .0624 | .0393 | .0344 | .0323 |
| 3 | .0480 | .0326 | .0357 | .0446 | .0329 | .0249 | .0473 | .0440 | .0338 | .0390 | .0504 | .0317 | .0317 |
| | .0729 | .0347 | .0283 | .0397 | .0344 | .0255 | .0427 | .0433 | .0301 | .0341 | .0483 | .0372 | .0310 |
| 4 | .0360 | .0412 | .0421 | .0317 | .0449 | .0430 | .0446 | .0341 | .0378 | .0283 | .0366 | .0427 | .0326 |
| | .0363 | .0378 | .0381 | .0289 | .0575 | .0433 | .0338 | .0437 | .0409 | .0277 | .0369 | .0412 | .0372 |
| 5 | .0366 | .0387 | .0437 | .0246 | .0212 | .0449 | .0424 | .0317 | .0363 | .0412 | .0249 | .0400 | .0741 |
| | .0347 | .0323 | .0320 | .0326 | .0366 | .0517 | .0452 | .0341 | .0387 | .0400 | .0421 | .0357 | .0430 |

- Réponse :

| i | $IC(Y^0, Y^i - k), 0 \leq k \leq 25$ | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | .0393 | .0452 | .0430 | .0366 | .0421 | .0341 | .0277 | .0243 | .0507 | .0384 | .0372 | .0350 | .0473 |
| | .0326 | .0344 | .0747 | .0246 | .0320 | .0323 | .0307 | .0360 | .0477 | .0464 | .0332 | .0369 | .0363 |
| 2 | .0332 | .0369 | .0430 | .0440 | .0273 | .0375 | .0320 | .0384 | .0409 | .0473 | .0381 | .0409 | .0329 |
| | .0338 | .0289 | .0440 | .0477 | .0280 | .0381 | .0344 | .0372 | .0458 | .0624 | .0393 | .0344 | .0323 |
| 3 | .0480 | .0326 | .0357 | .0446 | .0329 | .0249 | .0473 | .0440 | .0338 | .0390 | .0504 | .0317 | .0317 |
| | .0729 | .0347 | .0283 | .0397 | .0344 | .0255 | .0427 | .0433 | .0301 | .0341 | .0483 | .0372 | .0310 |
| 4 | .0360 | .0412 | .0421 | .0317 | .0449 | .0430 | .0446 | .0341 | .0378 | .0283 | .0366 | .0427 | .0326 |
| | .0363 | .0378 | .0381 | .0289 | .0575 | .0433 | .0338 | .0437 | .0409 | .0277 | .0369 | .0412 | .0372 |
| 5 | .0366 | .0387 | .0437 | .0246 | .0212 | .0449 | .0424 | .0317 | .0363 | .0412 | .0249 | .0400 | .0741 |
| | .0347 | .0323 | .0320 | .0326 | .0366 | .0517 | .0452 | .0341 | .0387 | .0400 | .0421 | .0357 | .0430 |

- $k_0 = k_1 - 15 \Rightarrow k_1 = k_0 + 15$
- $k_0 = k_2 - 22 \Rightarrow k_2 = k_0 + 22$
- $k_0 = k_3 - 13 \Rightarrow k_3 = k_0 + 13$
- $k_0 = k_4 - 17 \Rightarrow k_4 = k_0 + 17$
- $k_0 = k_5 - 12 \Rightarrow k_5 = k_0 + 12$
- 
  - 1er essai : $E_{k_0}(E) = Q \Rightarrow E_{k_0}(E) = Q \Rightarrow 4 + k_0 = 16 \Rightarrow k_0 = 12(M) \Rightarrow k_1 = 1(B); k_2 = 8(I); k_3 = 25(Z); k_4 = 3(D); k_4 = 24(Y)$. Décrypter $e_k(m)$ avec la cl $MBIZDY$ ne donne pas un message qui a un sens.
  - 2me essai : $E_{k_0}(E) = G \Rightarrow E_{k_0}(E) = G \Rightarrow 4 + k_0 = 6 \Rightarrow k_0 = 2(C) \Rightarrow k_1 = 17(R); k_2 = 24(Y); k_3 = 15(P); k_5 = 14(O)$. Décrypter $e_k(m)$ avec la cl $CRYPTO$ donne :
    I learned how to calculate the amount of paper needed for a room when i was at school. You multiply the square footage of the walls by the cubic contents of the floor and ceiling combined and double it. You then allow half the total for openings such as windows and doors. Then you allow the other half for matching the pattern. then you double the whole thing again to give a margin of error and then you order the paper.

## Cryptanayse du chiffrement de Veigenere : Test de Kasiski

- Q1 : Encrypter $m$= "THE CHILD IS FATHER OF THE MAN" avec la clé $k$="POETRY" en utilisant le chiffrement de Vigenere.
- R1 : $e_k(m)$=IVI VYGARMLWY IVI KFD IVIFRL
- Q2 : Appliquer le test de Kasiski sur le texte chiffré obtenu en (Q1) pour déduire la taille de la clé $k$.
- R2 : $e_k(m) = \underbrace{IVIVYGARMLWY}_{12}\underbrace{IVIKFD}_{6}IVIFRL$

$pgcd(6, 12) = 6$ donc il y a une forte chance que la clé soit 6 ou bien un diviseur de 6.