Master II RT.

Corrigé-type Epreuve : Cryptage.

Questions de Cours : (4pts).

Voir cours.

Exercice 1 : (3pts)

Soit le message : "CECI EST UN ESSAI DE VERITE"

→ On chiffre en utilisant la méthode de César avec ~~des~~ blocs de longueur = 4 ;

M = CECI ESTU NESS AIDE VERI TE AA

- les deux dernières lettres correspondant à la valeur "0" (zéro ajouté pour former le bloc de 4 lettres).
- On utilise les numéros de lettres selon l'intervalle $[0, 25]$.
- La clé est donnée $K = [K_1, K_2, K_3, K_4]$

$$K = [3, 1, 5, 2].$$

Numéro	2 4 2 8	4 18 19 20	13 4 18 18	~~VERI~~ 0 8 3 4
message	C E C I	E S T U	N E S S	A I D E
Clé K :	3 1 5 2	3 1 5 2	3 1 5 2	3 1 5 2

1

Numero	20 4 17 8	19 4 0 0
message	V E R I	T E A A
Clé	3 1 5 2	3 1 5 2.

→ Après utilisation de la loi : $C = (M + K) \bmod 26$

$\Rightarrow$ On obtient.

55 7 10 7 19 24 22 16 5 23 20 3 9 8 6

Chiffré : F F H K H T Y W Q F X V D J I G

23 5 22 10 22 5 5 2

X F W K W F F C.

1

$\Rightarrow$ donc le message chiffré et envoyé est :

"FFHKHTYWQFXVDJIGXFWKWFFC".

1

Exercice 2 : (5pts)

En utilisant la cryptanalyse du chiffrement Affine et en se basant sur l'analyse de fréquence des lettres.

1) $\Rightarrow$ $Q = 4$; $j = 12$, $w = 3 = N = X$.

donc $\begin{cases} f(E) = j & 4 \longleftrightarrow 9 \Leftrightarrow E \leftrightarrow J. \\ f(S) = Q & 18 \longleftrightarrow 16 \Leftrightarrow S \leftrightarrow Q. \end{cases}$

$\Rightarrow \begin{cases} f(4) = 9 \\ f(18) = 16. \end{cases}$

1

2) $(k_1, k_2) = ?$

En résolvant l'équation $(M.k_1 + k_2)$: message

$\Rightarrow \begin{cases} 4k_1 + k_2 \equiv 9 \pmod{26} \\ 18k_1 + k_2 \equiv 16 \pmod{26} \end{cases}$

1

avec les conditions : $\gcd(k_1, 26) = 1$,

et $k_1, k_2 \in [0, 25]$

$\Rightarrow 14k_1 \equiv 7 \bmod 26 \Rightarrow (14k_1 - 7) \bmod 26 = 1$

la valeur de k_1 qui verifie l'équation

est $\boxed{k_1 = 8}$ 1

$\Rightarrow$ On remplace : $4\underset{8}{k_1} + k_2 \equiv 9 \pmod{26}$

$\Rightarrow 36 + k_2 \equiv 9 \pmod{26}$

$\Rightarrow (k_2 + 27) \bmod 26 = 1.$

$\Rightarrow \boxed{k_2 = 26}$ 1

Remarque: $\gcd(k_1, 26) = \gcd(8, 26) \neq 1$

et en plus $k_2 \notin [0, 25]$

$\Rightarrow$ donc pas de solutions.

3) Pour l'équation dedéchiffrement :

$M_i = k_1^{-1}(C_i - k_2) \bmod 26$ 1

$\Rightarrow k_1^{-1} = ? \Rightarrow (k_1 \times ?) \bmod 26 = 1.$

$\Rightarrow$ pas de solution pour cet équation.
$(\gcd(k_1, 26) \neq 1).$

Exercice 3 : (5pts)

En utilisant le chiffrement RSA à clé publique (1943, 5)

Et en utilisant un chiffrage en bloc $(L = 2) \Rightarrow$ le message : "OKPOURSAMEDI"

devient :

$\overline{O\ K}$ $\overline{P\ O}$ $\overline{U\ R}$ $\overline{S\ A}$ $\overline{M\ E}$ $\overline{D\ I}$

14 10 15 14 20 17 18 00 12 04 03 08 (1)

le diagramme OK devient : $14 \cdot 26^1 + 10 = 374$

" PO " : $15 \cdot 26^1 + 14 = 404$.

.... Etc ...

• En utilisant la clé (1943, 5) :

	OK	PO	UR	SA	ME	DI
M	374	404	537	468	316	86
chiffré ∈ $C = M^5 \bmod (1943)$	1932	635	68	937	221	985

$\rightarrow C_{374} = (374)^5 \bmod (1943)$?

$(374)^2 \equiv 139876 \equiv 1923 \bmod (1943)$

$(374)^3 \equiv (374)^2 \cdot (374) \equiv 1923 \cdot 374 \equiv 292 \bmod (1943)$

$(374)^5 \equiv (374)^3 \cdot (374)^2 \equiv 292 \cdot 1923 \equiv 1932 \bmod (1943)$

$\Rightarrow \boxed{C_{374} = (374)^5 \bmod (1943) = 1932}$

2,5

$\rightarrow C_{537} = (537)^5 \bmod (1943) = ?$

$(537)^2 \equiv 288369 \equiv 805 \bmod (1943)$

$(537)^3 \equiv (537)^2 \cdot 537 \equiv 805 \cdot 537 \equiv 939 \bmod (1943)$

$(537)^5 \equiv (537)^2 \cdot (537)^3 \equiv 805 \cdot 939 \equiv 68 \bmod (1943)$

$\Rightarrow \boxed{C_{537} = (537)^5 \bmod (1943) = 68}$

... etc ...

⇒ le message chiffré en lettre :

1932 635 68 937 221 985

→ 1932 = $\underbrace{2}_{C} \cdot 26^2 + \underbrace{22}_{W} \cdot 26 + \underbrace{8}_{I}$ ⇔ CWI

→ 635 = $\underbrace{24}_{Y} \cdot 26^1 + \underbrace{11}_{L}$ ⇔ YL

→ 68 = $\underbrace{2}_{C} \cdot 26^1 + \underbrace{16}_{Q}$ ⇔ CQ.

1,5

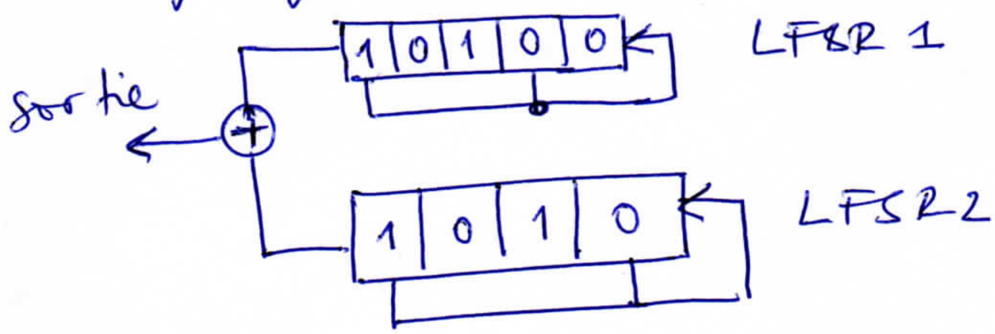
... etc ...

donc on obtient :

⟹ $\boxed{\text{CWI YL CQ BKB IN BLX.}}$

Exercice 4 : (3pts)

Soit le cryptage par flot basé sur deux LFSR :



1) La suite de sortie après 9 tops est :

000011101 (1)

cette suite est obtenue par un XOR entre les deux sorties des LFSRs :

LFSR1 : 1010001100 ⇒ on voit bien
LFSR2 : 1010111001 que N m

2) (1) Pour rendre la période la plus longue possible

3) (1) Si on continu dans les tops, on voit bien que l'état initial n'est pas obtenu qu'après plus de 25 tops. ⇒ le système est sécurisé (5)