Université 20 Août 1955, Skikda. **Responsable de la matière: Dj. ZEGHIDA.**
Département d'informatique. **Promotion : M1, Réseaux et Systèmes Distribués.**

Corrigé type de l'Examen de Moyenne Durée & Micro Interrogation du 05/06/2022.

Matière : Sécurité des Systèmes Informatiques.

Question 1 : (08 points)

1. Chiffrer avec ***Végenère*** , **M= SECURITE** et **k=FOX**.

Végenère	F	O	X					
M	S	E	C	U	R	I	T	E
Rang (p)	18	4	2	20	17	8	19	4
Clé	F	O	X	F	O	X	F	O
K_i	5	14	23	5	14	23	5	14
p + Ki	23	18	25	25	31	31	24	18
p + Ki mod (26)	23	18	25	25	5	5	24	18
C	X	S	Z	Z	F	F	Y	S

C= **XSZZF FYS** (04 points)

2. Chiffrer M= **HOLY** avec ***Hill*** , la clé : $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

Hill				
M	H	O	L	Y
Rang (p_i)	7	14	11	24
C_i	119	133	195	233
C_i mod (26)	15	3	13	15
C	P	D	N	D

$$\begin{pmatrix} C1 \\ C2 \end{pmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{pmatrix} 7 \\ 14 \end{pmatrix} = \begin{pmatrix} 9*7+4*14 \\ 5*7+7*14 \end{pmatrix}$$

$$= \begin{pmatrix} 63+56 \\ 35+98 \end{pmatrix} = \begin{pmatrix} 119 \\ 133 \end{pmatrix}$$

$$\begin{pmatrix} C3 \\ C4 \end{pmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{pmatrix} 11 \\ 24 \end{pmatrix} = \begin{pmatrix} 9*11+4*24 \\ 5*11+7*24 \end{pmatrix}$$

$$= \begin{pmatrix} 99+96 \\ 55+168 \end{pmatrix} = \begin{pmatrix} 195 \\ 233 \end{pmatrix}$$

C= **PDND** (04 points)

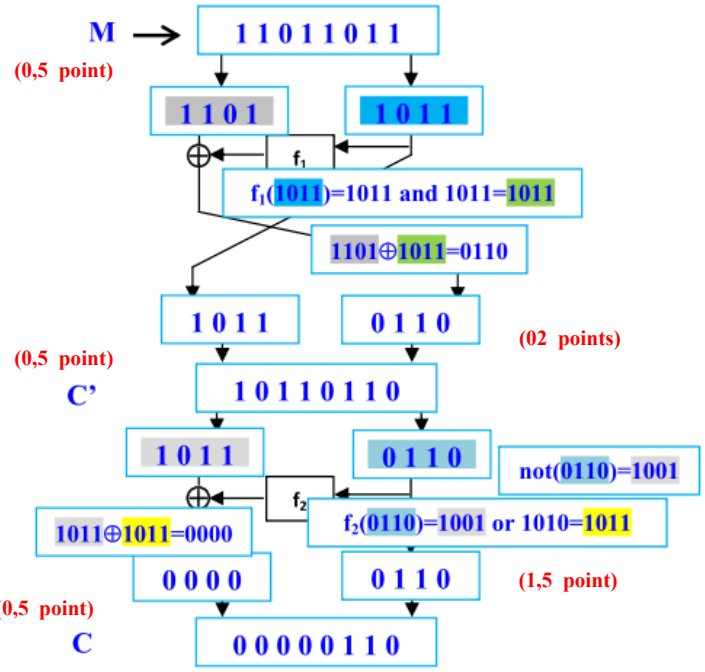
Question 2 : (12 points)

On a un réseau de ***Feistel*** à deux rondes sur des chaînes de 8 bits avec deux fonctions $\mathbf{f_1}$ et $\mathbf{f_2}$.

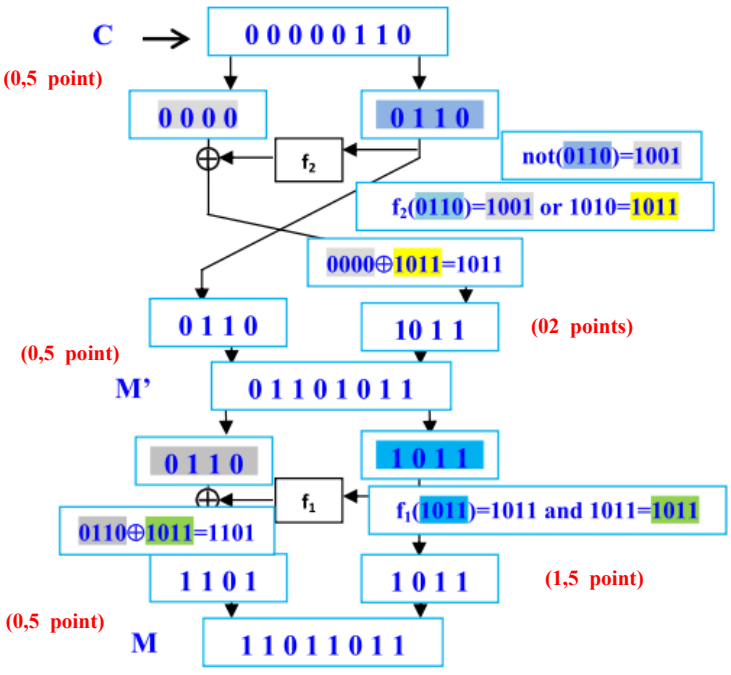
Pour toute chaîne **a** de 4 bits, on pose :

f_1(a)= a AND 1011, f_2(a)= NOT a OR 1010

M= **11011011**.



1° **Le premier réseau est pour le Chiffrement** (01 point)



2° **Le second réseau est pour le Déchiffrement** (01 point)