

MODULE 1: Sécurité & Cryptographie

Partie 1: Cryptographie

Les méthodes de chiffrage/
déchiffrement ('cryptographie')
qui peuvent être inclus dans
l'examen:

- 1)* • César ✓
- 2)* • Code de Vignère ✓
- 3)* • Code de Hill ✓
- 4)* • DES Modifié / DES simplifié ✓
- 5)* • Substitution mono-alphabétique ✓
- 6)* ~ Enigma cryptage ✓
- 7)* • cryptage Asymétrique RSA. ✓
- 8)*

Partie 2: Sécurité

BY ELMOUDEN /
NISRINE

1 - A1

1) chiffrement de César:

Cette méthode est basée sur le décalage par clé

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
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																			
23	24	25	26																			

c'est notre décalage ou clé (key) = 3
Exp: chiffre le mot "NISRINE"

Formule: $\Rightarrow X = (M + K) \bmod 26$

$$\begin{aligned} "NISRINE" &= (N + 3) \bmod 26 \\ &= (14 + 3) \bmod 26 \\ &= 17 \bmod 26 = 17 = Q \end{aligned}$$

$\hookrightarrow N \rightarrow Q$

$$\begin{aligned} "NISRINE" &= (I + 3) \bmod 26 \\ &= (9 + 3) \bmod 26 \\ &= 12 \bmod 26 = 12 = L \end{aligned}$$

$\hookrightarrow I \rightarrow L$

1) b) déchiffrement de César: " Extra ... "

Formule: $\Rightarrow X = (M - K) \bmod 26$

$$\begin{aligned} "QLVULQH" &= (Q - 3) \bmod 26 \\ &= (17 - 3) \bmod 26 \\ &= 14 = N \end{aligned}$$

$\hookrightarrow Q \rightarrow N$

c'est le déchiffrement

Extra ...

Code Vignère

١٢) الحروف من A=0

$\leftarrow \text{زیرا}$

A = 0 \rightarrow "Le message à chiffrer : " Cryptographie "

Lacle : " SMISSIX "

Message	C	R	Y	P	I	O	G	R	A	P	H	I	E
N_1^o	2	17	24	15	19	14	6	17	0	15	7	8	4
clé	S	M	I	S	S	I	X	S	M	I	S	S	I
N_2^o	16	12	8	18	18	8	23	18	12	8	18	18	8
$M_1^o + N_2^o$	2+18 20	17+12 29	24+8 32	15+18 33	19+18 37	14+8 22	6+23 29	17+18 35	0+12 12	15+8 23	7+18 25	8+18 26	4+8 12
Resultat	U	D	G	H	L	W	D	j	M	X	Z	A	M

2-) b) le déchiffrement de Vignère:

Case 1: on sait l'aclé

Alors pour le message déchiffré : "UDGHLWDjMXZAM" avec la clé : "MISSIX"

Alors pour le message avec l'addé : "SMISSIX"													
L	U	D	G	H	L	W	D	j	M	X	Z	A	M
20	29	32	33	37	22	29	29	35	12	23	25	26	12
S	M	I	S	S	I	X	S	M	I	S	S	I	8
18	12	8	18	18	8	23	18	12	8	18	18	18	8
20-18	29-19	32-8	33-18	37-18	22-8	29-23	35-18	12-12	23-8	25-18	26-18	12-8	4
C	Y	P	T	O	9	9	9	a	P	F	8	i	e

3-a) chiffrement de Hill cipher

B-C₂

Encryption

Formule

$$\Rightarrow C = E(K, P) = P \times K \bmod 26$$

K est une matrice

Algo
Hill

$$(C_1 \ C_2 \ C_3) = (P_1 \ P_2 \ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$C_1 = (P_1 K_{11} + P_2 K_{21} + P_3 K_{31}) \bmod 26$$

$$C_2 = (P_1 K_{12} + P_2 K_{22} + P_3 K_{32}) \bmod 26$$

$$C_3 = (P_1 K_{13} + P_2 K_{23} + P_3 K_{33}) \bmod 26$$

Ex: si notre (key) $K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

Encrypt "Pay more money"

on a $K = 3 \times 3$ matrice

Alors $P = \begin{pmatrix} \text{Pay} \\ \text{more} \\ \text{money} \end{pmatrix}$

on appliquant Algo de Hill :

Pay :

←	P	A	Y	m	o	r	e	m	o	n	e	y
	15	0	24	12	14	17	4	12	14	13	4	24

$$(C_1 \ C_2 \ C_3) = (15 \ 0 \ 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$\begin{aligned}
 &= (15 \times 17 + 0 \times 21 + 24 \times 2) \ 15 \times 17 + 0 \times 18 + 24 \times 2 \ 15 \times 5 + 0 \times 21 + \\
 &\quad 24 \times 19 \bmod 26 \\
 &= (303 \ 303 \ 531) \bmod 26 = (17 \ 17 \ 11) \\
 &\quad = (R \ R \ L) \checkmark
 \end{aligned}$$

mod?

$$\begin{aligned} (C_1 C_2 C_3) &= (12 \ 14 \ 17) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{mod } 26 \\ &= (12 \times 17 + 14 \times 21 + 17 \times 2 \quad 12 \times 17 + 14 \times 18 + 17 \times 2 \\ &\quad 12 \times 5 + 14 \times 21 + 17 \times 19) \text{mod } 26 \\ &= (532 \ 490 \ 677) \text{mod } 26 \\ &= (12 \ 22 \ 1) \\ &= (M \ W \ B) \end{aligned}$$

B - C₂

" " " Extra...
(emo ney)

pay more money
RRL MWBK ASPDH

سکه
نیزیل



3. b) déchiffrement de Hill cipher

3-6

Decryption
Formule

$$P = D(K, C) = CK^{-1} \bmod 26$$

ou bien

$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adj } K$$

l'inverse
de la matrice
K.

Exp: si notre (key) $K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

Décrypt "RRLMWBKASPEDH"

on appliquant Algo de Hill:

Det K

$$\text{on a } K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \xrightarrow{\text{adj}} \begin{pmatrix} + & - & + \\ - & + & - \\ + & - & + \end{pmatrix}$$

الخطوة 1 :

$$\textcircled{1} \quad \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

$$\textcircled{2} \quad \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

$$\textcircled{3} \quad \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

$$\begin{aligned} \Rightarrow \text{Det } K &= \text{Det} \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} = +17 \cdot (18 \times 19 - 2 \times 21) - \\ &17(19 \times 21 - 2 \times 21) + 5(21 \times 2 - 2 \times 18) \bmod 26 = \\ &(+17(342 - 42) - 17(399 - 42) + 5(42 - 36)) \\ &\bmod 26 = (5100 - 6069 + 30) \bmod 26 = -939 \bmod 26 = 3 \bmod 26 = 23 \end{aligned}$$

Along Det K = 23

3-C 4

Adj K

$$\text{Adj } K = \text{Adj}$$

صيغة - 2
لعدد ماتابع العمودين

$$\begin{vmatrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{vmatrix}$$

نجد ماتابع السطر بين

$$= \begin{vmatrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{vmatrix}$$

$$\text{Adj } K =$$

$$18 \times 19 - 2 \times 21$$

$$2 \times 5 - 17 \times 19$$

$$17 \times 21 - 18 \times 5$$

$$21 \times 2 - 19 \times 21$$

$$19 \times 17 - 5 \times 2$$

$$5 \times 21 - 21 \times 17$$

$$21 \times 9 - 2 \times 18$$

$$2 \times 17 - 17 \times 2$$

$$17 \times 18 - 21 \times 17$$

$$\begin{pmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{pmatrix} \mod 26$$

$$\begin{pmatrix} 14 & -1 & 7 \\ -19 & 1 & -18 \\ 6 & 0 & -25 \end{pmatrix} \mod 26$$

$$\text{Adj } K = \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \begin{pmatrix} -19 \mod 26 & 7 \\ 26 - 19 = 7 \\ -18 \mod 26 & 8 \\ 26 - 18 = 8 \end{pmatrix}$$

$$\text{Adj } K = \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix}$$

كما في المثلث

$$\text{Det } K = 23 \quad 9$$

$$K^{-1} = \frac{1}{\det K} \times \text{Adj } K$$

ومنها

3-C-5

$$K^{-1} = \frac{1}{23} \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \mod 26 \quad C=1$$

$$K^{-1} = 23^{-1} \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \mod 26.$$

on cherche $23^{-1} \mod 26$

$$\text{on a } 23^{-1} \times 23 = 1 \mod 26$$

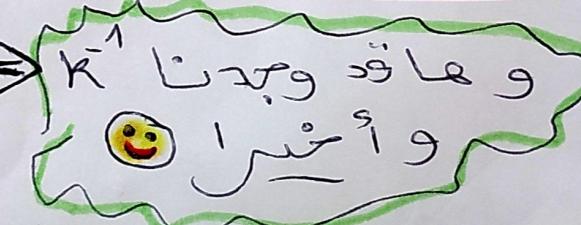
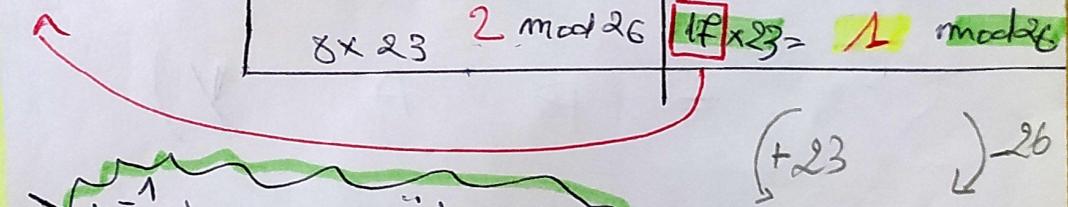
$$y = x - 26k \leq ? \times 26 \Leftarrow +23$$

$$K^{-1} = 17 \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 202 & 0 & 17 \end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

$23^{-1} \times 23 = 1 \mod 26$	$9 \times 23 = 25 \mod 26$
$1 \times 23 = 23 \mod 26$	$10 \times 23 = 22 \mod 26$
$2 \times 23 = 20 \mod 26$	$11 \times 23 = 19 \mod 26$
$3 \times 23 = 17 \mod 26$	$12 \times 23 = 16 \mod 26$
$4 \times 23 = 14 \mod 26$	$13 \times 23 = 13 \mod 26$
$5 \times 23 = 11 \mod 26$	$14 \times 23 = 10 \mod 26$
$6 \times 23 = 8 \mod 26$	$15 \times 23 = 7 \mod 26$
$7 \times 23 = 5 \mod 26$	$16 \times 23 = 4 \mod 26$
$8 \times 23 = 2 \mod 26$	$17 \times 23 = 1 \mod 26$



الخطوة الرابعة
النتائج لفك التشفرة

$$P = C K^{-1} \mod 26$$

لدينا ندخل بعد الحروف مابين:

R	R	L	M	W	B	K	A	S	P	D	H
17	17	11	12	22	1	10	0	18	15	3	7

RRL:

3 - C6

$$(P_1 P_2 P_3) = (RRL) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \text{ mod } 26$$

$$= (17 \times 1 + 17 \times 11) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \text{ mod } 26$$

$$= (17 \times 4 + 17 \times 15 + 11 \times 24) \quad 17 \times 9 + 17 \times 17 + 11 \times 0$$

$$= (17 \times 15 + 17 \times 6 + 11 \times 17) \text{ mod } 26$$

$$= (587 \quad 442 \quad 544) \text{ mod } 26.$$

$$= (15 \quad 0 \quad 24)$$

$$= (P \quad A \quad Y)$$

MWB:

= = = Extra

RRL MWBK ASPDH
Pay money money

بندقية
الشمير



4-a) chiffrement par substitution Mono₂ (H-D₂)

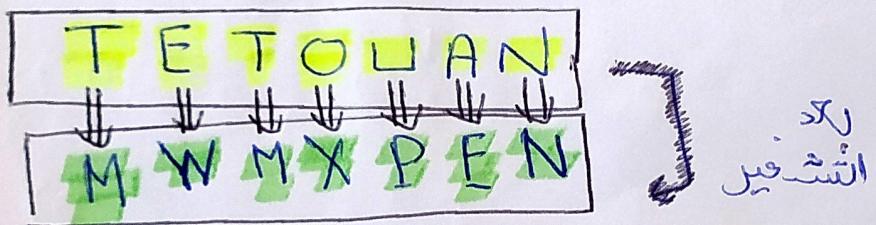
Alphabétique :

* تاتي هذه التقنية باعادة ترتيب حرف بشكل عشوائي (يعني اختياري) :

Exp:

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
E	Y	F	Q	W	D	T	C	R	J	B	G	A	N	X	O	I	L	Z	M	P	S	H	K	V	U

ملاحظة: في حالة استخدامنا لحرف في التشفير فلن ينفعه الخوارزمية لاستخدام الحرف الذي يليه * لذا نتغير لفمة "TETOUAN" الى "TETOUAN" الجدول الشهوانى أعلاه.



5) ^a- chiffrement (cryptage) Asymétrique RSA

5-E_n

نختار رقمي عشوائيين أوليين (1
أو يتم إعطاؤهما في التعريف) Pg 9

$n = p \times q$: RSA Modulus : (جذر متعال) (٢)

$$\phi(n) = (p-1) \times (q-1)$$

زخم = α Euler بالخطوة الثالثة:

$$n < e < \epsilon(n) \quad \text{avec } n \text{ un exposant}$$

$$\operatorname{pgcd}(e, \phi(n)) = 1$$

اتصل على message الـ **شغف** و **الحب** (5)

$$C = M^e \bmod n \Rightarrow$$

* Exp: chiffrer le message "HIDE"

ona $H=7$, $I=8$, $D=3$, $E=4$.

et on a $C = ne \pmod{n}$ \Rightarrow c'est l'équation de chiffrement de chaque lettre

onchoisis, $P=11$ et $q=5$ \Rightarrow Alors $n = p \times q = 55$ et ~~on voit~~ message.

Lettre	Valeur numérique	chiffre de la lettre
H	7	$C = 7^F \pmod{55} = 28 \pmod{55}$
I	8	$C = 8^F \pmod{55} = 2 \pmod{55}$
D	3	$C = 3^F \pmod{55} = 42 \pmod{55}$
E	4	$C = 4^F \pmod{55} = 49 \pmod{55}$

28, 2, 42, 49

$$\cancel{m \neq e = f} \Rightarrow \text{such } p \text{ gcd}(f, 40) = 1, 1 < f < 40$$

b) Déchiffrement RSA:

5-E3

$$M = C^D \bmod n$$

Decryption
Formule

$$D = e^{-1} \bmod \varphi$$

ExP:

le message "

" 28, 2, 42, 49 "

$$\varphi(n) = 40 \quad \rightarrow \quad e = f$$

$$\rightarrow D = f^{-1} \bmod 40$$

$$D \times f = 1 \bmod 40$$

تُعَدِّل

D \rightarrow تردد



نحوك تُسْخِنْ

لدينا

Algorithme d'Euclide

Algorithme d'Euler Etendu

le résultat

$$40 = 5 \times f + 5$$

$$f = 1 \times 5 + 2$$

$$5 = 2 \times 2 + 1$$

on s'arrête au dernier reste non nul.

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - 2 \times (f - 1 \times 5) \\ &= 5 - 2 \times f + 2 \times 5 \\ &= 3 \times 5 - 2 \times f \\ &= 3 \times (40 - 5 \times f) - 2 \times f \\ &= 3 \times 40 - 15 \times f - 2 \times f \\ &= 3 \times 40 + (-17) \times f \end{aligned}$$

on alors nos valeurs négatives
40 et f

si le coefficient est
positif ce nombre
sera notre clé de
chiffrement, mais
 -17 est négatif
on doit calculer:

$$d = -17 \pmod{40}$$

$$d = 23 \pmod{40}$$

$$(40 - 17 = 23)$$

Alors 23 est notre
clé

$$M = C^D \pmod{n}$$

Code	Le déchiffrement de lettre		lettre correspondante
28	$28^{23} \pmod{55}$	$\rightarrow 7 \pmod{55}$	H
2	$2^{23} \pmod{55}$	$\rightarrow 8 \pmod{55}$	I
42	$42^{23} \pmod{55}$	$\rightarrow 3 \pmod{55}$	D
49	$49^{23} \pmod{55}$	$\rightarrow 4 \pmod{55}$	E

privées

publiques

هذه المنهجية: هنا كل من الفضل
اعلن يقوم بتحديد جميع العوائق قبل التسليم والتحقق
من صحة الرياح

P	q	e(n)	d	n	e
11	5	40	23	55	7

le % mod (الرقم المتبقي %)

5-E₃

Méthode ①

pour le code 28 $\Rightarrow 28^{23} \pmod{55}$

$$28^2 = 784 \pmod{55}$$

$$28^4 = 14 \pmod{55}$$

$$28^2 \times 28^2 = 14 \times 14 \pmod{55}$$

$$\hookrightarrow 28^4 = 196 \pmod{55}$$

$$28^4 = 31 \pmod{55}$$

$$28^2 \times 28^4 = 14 \times 31 \pmod{55}$$

$$28^6 = 434 \pmod{55}$$

$$28^6 = 49 \pmod{55}$$

$$28^6 \times 28^4 = 49 \times 31 \pmod{55}$$

$$28^{10} = 1519 \pmod{55}$$

$$28^{10} = 34 \pmod{55}$$

$$28^{10} \times 28^{10} = 34 \times 34 \pmod{55}$$

$$28^{20} = 1156 \pmod{55}$$

$$28^{20} = 1 \pmod{55}$$

$$28^{20} \times 28^2 = 1 \times 14 \pmod{55}$$

$$28^{22} = 14 \pmod{55}$$

$$28^{22} \times 28 = 14 \times 28 \pmod{55}$$

$$28^{23} = 392 \pmod{55}$$

$$28^{23} = 17 \pmod{55}$$

on a A mod B (par calculatrice)

$$\textcircled{1} \quad A / B = C$$

$$\textcircled{2} \quad C * B = E$$

$A - E =$ le reste final

Méthode ②

" " " " $\Rightarrow 28^{23} \pmod{55}$

$$M = 28$$

$$d = 23 \Rightarrow$$

$d = 1$ (First)

$d^2 \Rightarrow$ if binary 0

$d^2 \times M \Rightarrow$ if binary 1

$$d = 23$$

to binary

128	64	32	16	8	4	2	1
				1	0	1	1

$$d = 23 \Rightarrow 10111$$

1	0	1	1	1
12	28^2	14^2	43^2	14^2
(mod 55)	784	196	1849	289
21×28 (mod 55)	$(mod 55)$	$(mod 55)$	$(mod 55)$	$(mod 55)$
$d = 38$	$d = 14$	31×28	34×28	14×28
		868 (mod 55)	952 (mod 55)	392 (mod 55)
		$d = 43$	$d = 17$	$d = 7$
		même résultat		

EXP: 784 mod 55

$$\textcircled{1} \quad 784 / 55 = 14$$

$$\textcircled{2} \quad 14 \times 55 = 770$$

$$\textcircled{3} \quad 784 - 770 = 14$$

6) a) chiffrement DE S- Modifié

6 - F₁

1) On a dans cette méthode :

a) la clé principale $\Rightarrow (a, b, U_0)$

b) les clés secondaires $\Rightarrow U_n$ tel que

$$U_{n+1} = a \times U_n + b$$

c) la taille du bloc (8 bites)

d) les addition (modulo 27 $L_i L_i'$)

e) le nombre d'itérations (2, 3, ... bites)

{ (b) \Rightarrow $U_0, U_1, U_2, U_3, U_4, U_5, U_6, U_7$ }
 { (les clés secondaires U_n) يجب حسابها }

$$M_{i+1} = [R_i \parallel k_i + g(i)]$$

Exp: [Rotation] [clé] [la moitié de Bloc après rotation]

on fait le chiffrement du message suivant

" COURS DE CRYPTOGRAPHIE "

a) on a la clé principale est $= (a, b, U_0) = (1, 3, 2)$

b) on calcule les clés secondaires on a $U_0 = 2$

$$U_{n+1} = a \times U_n + b \Rightarrow$$

c) la taille de bloc est : 8

d) les addition modulo : 27

e) le nombre d'itérations est : 2

on a 2 itérations

$$\begin{cases} U_0 = 2 \\ U_1 = 1 \times 2 + 3 = 5 \\ U_2 = 1 \times 5 + 3 = 8 \\ U_3 = 1 \times 8 + 3 = 11 \end{cases}$$

$$\begin{cases} U_4 = 1 \times 11 + 3 = 14 \\ U_5 = 1 \times 14 + 3 = 17 \\ U_6 = 1 \times 17 + 3 = 20 \\ U_7 = 1 \times 20 + 3 = 23 \end{cases}$$

Plus \Rightarrow 2 clés (k_1, k_2)

ما يجب
معرفته
قبل الالتحاق
لـ الطريقة

⇒ COURS DE CRYPTOGRAPHIE

6-F₂)

3 15 21 18, 19 0 45, 0 3 18 25 16 20 15 7 18 1 16 8 9 5
Gg Dd

$$M_0 = [\begin{matrix} 3 & 15 & 21 & 18 & 11 & 19 & 0 & 4 & 5 \end{matrix}]$$

$$\begin{array}{r}
 19 \quad 0 \quad 4 \quad 5 \\
 \text{Permutation 1} \\
 \begin{array}{c}
 1 \\
 \oplus \quad U_0 \quad U_1 \quad U_2 \quad U_3 \\
 \hline
 15 \quad 21 \quad 18 \quad 3 \quad (\text{Rotation 1})
 \end{array} \\
 \begin{array}{c}
 \text{ajoute de} \\
 \text{l'addition} \\
 \text{F1}
 \end{array}
 \end{array}$$

$$M_1 = \begin{bmatrix} 19 & 0 & 45 \\ & \overbrace{\hspace{1cm}}^G_1 & \overbrace{\hspace{1cm}}^{D_1} \\ 17 & 26 & 26 & 14 \end{bmatrix}$$

$$\begin{array}{r}
 17 \ 26 \ 26 \ 14 \quad \text{permutation 2} \quad 0 \ 4 \ 5 \ 19 \quad (\text{rotation } 9) \\
 \oplus \quad U_4 \ U_5 \ U_6 \ U_7 \\
 \hline
 0 \ 4 \ 5 \ 19 \\
 \oplus \quad 14 \ 17 \ 20 \ 23 \\
 \hline
 14 \ 21 \ 25 \ 15
 \end{array}$$

ajoute de la clé **K2**

$$M_{12} = [17 \ 26 \ 26 \ 14 \quad 14 \ 21 \ 25 \ 15]$$

Mn = Q Z Z N N U Y O

la même chose pour les autres blocs
- "permutation" - "rotation" - "ajout de la clé" - "inverse"