Université Abbes Laghrour -Khenchela, Département Infor

Exo1=...../5, Exo2=...../5, Exo3=...../5, Exo4=...../5

.....
20

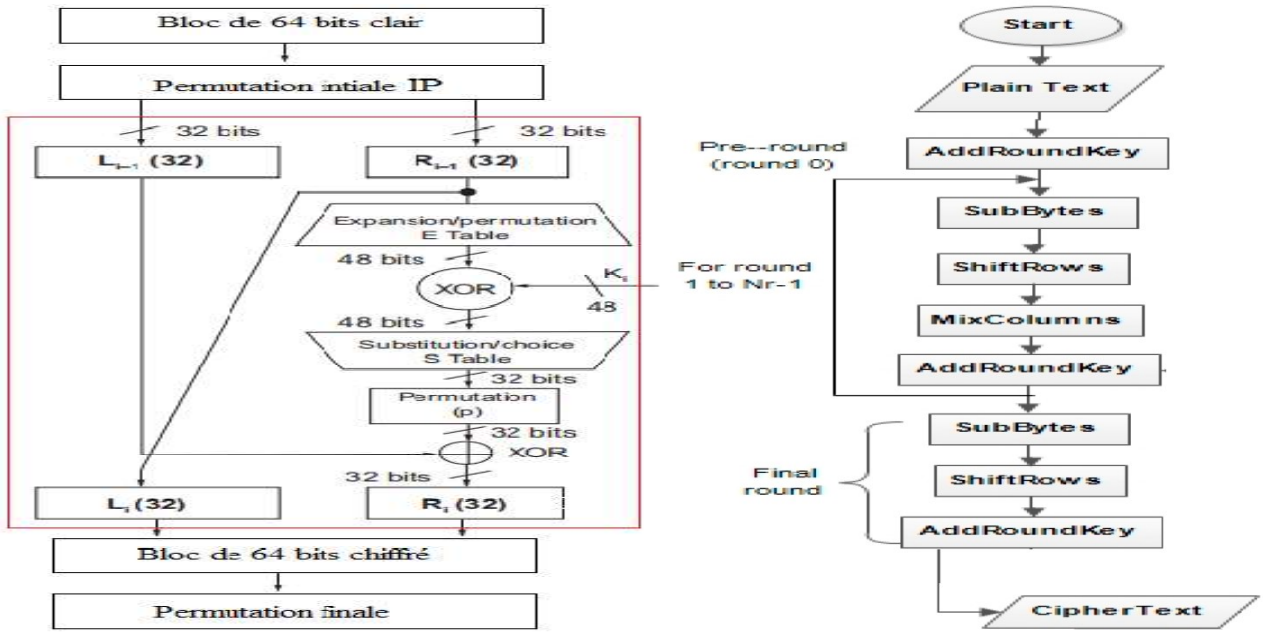
Nom :.....

Prénom :.....

Master 1 **SI** **cryptographie et sécurité** (solution) **18/05/2025, 1h30mn**

Exercice 1 (5 points):

Question1 (2.5 points): Complétez les diagrammes suivants de DES et AES.



Question 2 (2.5 points): Générez la première clé K_1 à partir de la clé K_0 en utilisant AES, en complétant le tableau suivant. Complétez uniquement les cases contenant des points. Détaillez votre réponse.

K_0				
	4A	7D	5B	F2
	3F	0E	6C	11
	8B	9A	D4	34
	1C	2F	E0	56

K_1			
C9	B4		
27			
3A			
95	BA		

1. Extraction de la dernière colonne (Colonne 3)[F2, 11, 34, 56]
2. RotWord([F2, 11, 34, 56])= [11, 34, 56, F2]
3. SubWord ([11, 34, 56, F2])= [82, 18, B1, 89]
4. Rcon(1) = [01, 00, 00, 00] XOR [82, 18, B1, 89]= [83, 18, B1, 89]
5. Génération des nouvelles colonnes :[4A,3F,8B,1C] XOR [83,18,B1,89] = [C9,27,3A,95]

Colonne 0 (nouvelle) :[4A,3F,8B,1C] XOR [83,18,B1,89] = [C9,27,3A,95], Colonne 1 :[7D,0E,9A,2F] XOR [C9,27,3A,95] = [B4,29,A0,BA], Colonne 2 :[5B,6C,D4,E0] XOR [B4,29,A0,BA] = [EF,45,74,5A], Colonne 3 :[F2,11,34,56] XOR [EF,45,74,5A] = [1D,54,40,0C]

Exercice 2(5 points):

1. Soit un registre à décalage à rétroaction linéaire (**LFSR**) de longueur 3 bits, utilisant la fonction de rétroaction : $F(x) = x_1$ XOR x_3. Le registre est initialisé avec l'état 001.Générez les trois prochaines valeurs de sortie du registre.

2. Chiffrez manuellement le message suivant à l'aide de l'algorithme RC4 : p = [9, 3, 1, 2]. La séquence S est de taille 4. La clé K est générée à partir des trois états successifs du LFSR, c'est-à-dire : K = [**valeur à l'horloge 1**, **valeur à l'horloge 2**, **valeur à l'horloge 3**].

Réponse:

LFSR

Horloge	Etat du LFSR	Sortie	K (en decimal)
0	001		
1	100	1	4
2	110	0	6
3	111	0	7

(1) Initialisation

S	T
0	4
1	6
2	7
3	4

(2) permutation initiale

i	j	S0	S1	S2	S3
	0	0	1	2	3
0	0	0	1	2	3
1	3	0	3	2	1
2	0	2	3	0	1
3	1	2	1	0	3

(3) Génération du flux

i	j	t	k	S0	S1	S2	S3
0	0			2	1	0	3
1	1	2	0	2	1	0	3
2	1	1	0	2	0	1	3
3	0	1	0	3	0	1	2
0	3	1	0	2	0	1	3

C=p⊕k= [9 3 1 2] ⊕ [0 0 0 0]= [1001, 0011, 0001, 0010] ⊕[0000, 0000, 0000, 0000] = [1001, 0011, 0001, 0010]= [9 3 1 2]

Exercice 3(5 points):

Alice souhaite recevoir des messages chiffrés au moyen d'un crypto-système d'ElGamal. Elle choisit pour cela: p = 17 et $\alpha = 5$ et une clé secrète d = 11.

1. Donner la clé publique d'Alice.

$\beta=\alpha^d \bmod p=5^{11} \bmod 17=11$, **Clé publique complète :**Le triplet (p,α,β) =(17,5,11)

Bob génère un nombre aléatoire k, k = 7. En suite, il veut transmettre M= 13, en calculant le cryptogramme *r*, *t*.

2. Donner la valeur de *r* et *t*.

$r=\alpha^k \bmod p=5^7 \bmod 17 =10$

$t=M\times\beta^k \bmod p=13\times11^7 \bmod 17= 5$

Alice reçoit le cryptogramme ElGamal ($r = 10$, $t = 10$).

3. Déterminer le message en clair correspondant.

$M=t\times r^{(p-1-d)} \bmod p=10\times10^{(17-1-11)} \bmod 17=10\times10^5 \bmod 17$

M=9

Exercice 4 (5 points):

Soient p = 7 et la courbe elliptique E: $y^2 = x^3 + 3x + 1$ sur le corps fini GF(7). On est donc dans $E_7(3, 1)$. Avec un point de base G(3,3) et une clé privée, n = 4:

1. Calculer (3,3)+ (3,3) puis (3,3)+(2,6), en utilisant la formule suivante:

Si P = (xP , yP) et Q = (xQ, yQ) avec P ≠ −Q, alors on détermine R = P + Q = (xR, yR) comme suit :

$$x_R = \left(\lambda^2 - x_P - x_Q\right) mod\ p$$
$$y_R = (\lambda\ (x_P - x_R) - y_P)\ mod\ p$$

Où $\lambda = \begin{cases} \left(\frac{y_Q - y_P}{x_Q - x_P}\right) mod\ p\ si\ P \neq Q \\ \left(\frac{3x_P^2 + a}{2y_P}\right)\ mod\ p\ si\ P = Q \end{cases}$

(3,3)+ (3,3) =(5,1) (0,5) points

(3,3)+(2,6)=(4,0) (0,5) points

2. Calculer la clé publique Q correspondant à la clé privée **n**.

$Q=n\cdot G=4\cdot G$

$Q=(6,2)$

3. Chiffrer le message M= (6,5) en utilisant la clé publique Q. Choisir un entier aléatoire k = 5 et calculer les points C_1 et C_2.

$(C1,C2)=(k\cdot G, M+k\cdot Q)$.

C1=5·G =(2,6)

C2=M+5·Q=(6,2)

(C1,C2)=((2,6),(6,2))

4. Déchiffrer ce message [(0,1),(4,0)] en utilisant la clé privée n et k=3.

M= C_2-[nC_1] =(4,0)-4.(1,0)

M=(4,0)

+	∞	(0,1)	(0,6)	(2,1)	(2,6)	(3,3)	(3,4)	(4,0)	(5,1)	(5,6)	(6,2)	(6,5)
∞	∞	(0,1)	(0,6)	(2,1)	(2,6)	(3,3)	(3,4)	(4,0)	(5,1)	(5,6)	(6,2)	(6,5)
(0,1)	(0,1)	(4,0)	∞	(5,6)	(6,5)	(6,2)	(5,1)	(0,6)	(2,6)	(3,3)	(2,1)	(3,4)
(0,6)	(0,6)	∞	(4,0)	(6,2)	(5,1)	(5,6)	(6,5)	(0,1)	(3,4)	(2,1)	(3,3)	(2,6)
(2,1)	(2,1)	(5,6)	(6,2)	(5,1)	∞	(6,5)	(4,0)	(3,3)	(0,6)	(2,6)	(3,4)	(0,1)
(2,6)	(2,6)	(6,5)	(5,1)	∞	(5,6)		(6,2)	(3,4)	(2,1)	(0,1)	(0,6)	(3,3)
(3,3)	(3,3)	(6,2)	(5,6)	(6,5)	(4,0)		∞	(2,1)	(0,1)	(3,4)	(2,6)	(0,6)
(3,4)	(3,4)	(5,1)	(6,5)	(4,0)	(6,2)	∞	(5,6)	(2,6)	(3,3)	(0,6)	(0,1)	(2,1)
(4,0)	(4,0)	(0,6)	(0,1)	(3,3)	(3,4)	(2,1)	(2,6)	∞	(6,5)	(6,2)	(5,6)	(5,1)
(5,1)	(5,1)	(2,6)	(3,4)	(0,6)	(2,1)	(0,1)	(3,3)	(6,5)	(6,2)	∞	(4,0)	(5,6)
(5,6)	(5,6)	(3,3)	(2,1)	(2,6)	(0,1)	(3,4)	(0,6)	(6,2)	∞	(6,5)	(5,1)	(4,0)
(6,2)	(6,2)	(2,1)	(3,3)	(3,4)	(0,6)	(2,6)	(0,1)	(5,6)	(4,0)	(5,1)	(6,5)	∞
(6,5)	(6,5)	(3,4)	(2,6)	(0,1)	(3,3)	(0,6)	(2,1)	(5,1)	(5,6)	(4,0)	∞	(6,2)

S-Box

hex		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	e5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	e7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fe	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	60	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0e	13	ee	5f	97	44	17	e4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	6e	22	2a	90	88	46	ee	b8	14	6e	5e	05	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6e	56	f4	ea	65	7a	be	08
	c	ba	78	25	2e	1e	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	cf	b0	54	bb	16