A

السؤال الأول : بفرض أن الخوارزمية RC4 تستخدم شعاع S مكون من 5 بايت، و مفتاح الدخل K=[3 12 15]

والمطلوب:

1. اكتب شعاع التهيئة S .
2. اكتب الشعاع T و علل إجابتك(دون كتابة الخوارزمية).
3. بفرض أن ناتج الـ Iteration 5 هو j=4, S={2,3,1,0,4} شفر النص الصريح P=AD .

Char	Dec	Char	Dec	Char	Dec
@	64	D	68	H	72
A	65	E	69	I	73
B	66	F	70	J	74
C	67	G	71	K	75

السؤال الثاني : في خوارزمية DES لدينا :

$$C_9=1111110011110001111001111110$$
$$D_9=1111001000111111111111111111$$

المطلوب:1. حدد رقم الحلقة المفروضة . مع التعليل

2 . احسب المفتاح الجزئي لهذه الحلقة .

A

السؤال الأول : (6.5)

1. شعاع التهيئة S : S={0,1,2,3,4}

2 . اكتب الشعاع T :

T= =[3 12 15 3 12]

التعليل: T له نفس طول S ، و محتواه مكونات المفتاح k .

3..من فرض المسألة لدينا ناتج الـ Iteration 5 هو S={2,3,1,0,4} ومنه نبدأ:

سلسلة المفتاح الأولى:

/* Stream Generation */

Reset i = j = 0, Recall S = {2,3,1,0,4}

i = (i + 1) mod5 = 1

j = (j + S[i])mod 5 = (0 + 3) mod 5 = 3

Swap S[i] and S[j], Swap S[1] with S[3]: S = {2,0,1,3,4}

Output K = S[(S[i] + S[j])mod 5] = S[(0+3)mod 5] = S[3]=3

$A=(65)_{10}=(01000001)_2$

0	1	0	0	0	0	0	1	
0	0	0	0	0	0	1	1	$\oplus$
0	1	0	0	0	0	1	0	=66
								=B

سلسلة المفتاح الثانية:

i = 1,j = 3, RecalL: S = {2,0,1,3,4}

i = (1 + 1) mod5 = 2

j = (3 + 1) mod 5 = 4

Swap S[2] and S[4]: S = {2,0,4,3,1}

Output K = S[(S[2] + S[4])mod 5]= S[(4+1)mod 5] = S[0]=2

$D=(68)_{10}=(01000100)_2$

0	1	0	0	0	1	0	0	
0	0	0	0	0	0	1	0	⊕
0	1	0	0	0	1	1	0	=70
								=F

➔ C=BF

A

السؤال الثاني(3.5) : المطلوب:1. رقم الحلقة =10 ، التعليل: i=10 ➔ i-1=9

2 . نتبع الخطوات الآتية :

1. نجري إزاحة دورانية إلى اليسارلكل من C, D بمقدار خانتين (من جدول التدوير) فيكون:

$$C_9=1011111100111100011110011111$$

$$D_9=1111110010001111111111111111$$

2. نلصق C9D9 بعد الإزاحة فيكون كالآتي (وهو دخل PC2)

$$C_9D_9= 1011111100111100011110011111\ 1111110010001111111111111111$$

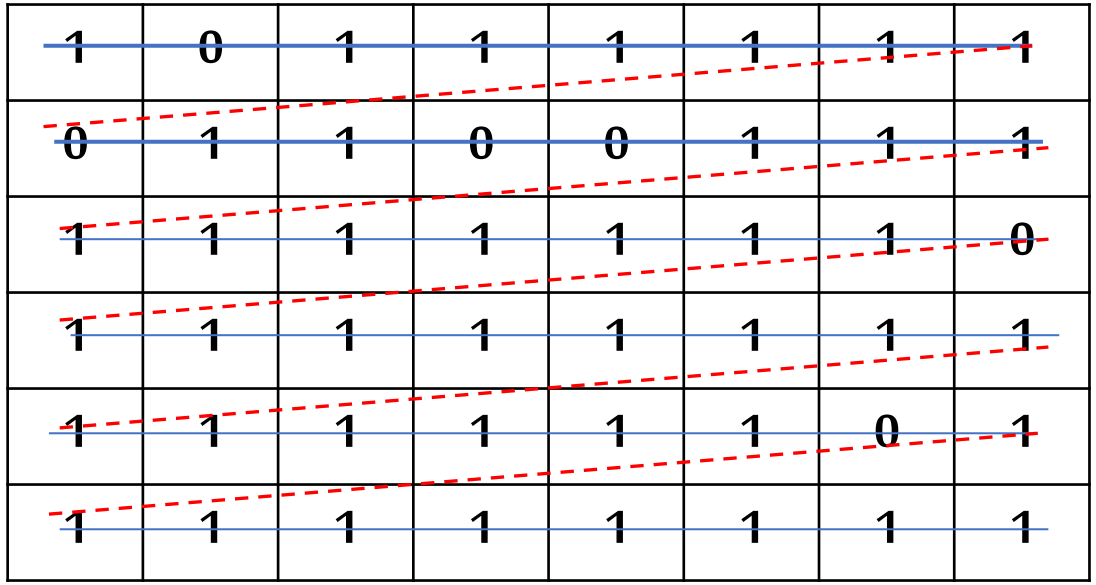
2. نستخدم جدول PC2 فيكون : 1. نرقم الخانات

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
1	0	1	1	1	1	1	1	0	0	1	1	1	1	0	0	0	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	0	0	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

A

2. نستخدم جدول PC2 فيكون : 2. نطبق الجدول ثم نجري مسح ZIGZAG

1	0	1	1	1	1	1	1
0	1	1	0	0	1	1	1
1	1	1	1	1	1	1	0
1	1	1	1	1	1	1	1
1	1	1	1	1	1	0	1
1	1	1	1	1	1	1	1



فيكون مفتاح الحلقة :

K10= 1 0 1 1 1 1 1 1 0 1 1 0 0 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1

B

السؤال الأول : بفرض أن الخوارزمية RC4 تستخدم شعاع S مكون من 4بايت، و مفتاح الدخل K=[7 11] والمطلوب:

Char	Dec	Char	Dec	Char	Dec
@	64	D	68	H	72
A	65	E	69	I	73
B	66	F	70	J	74
C	67	G	71	K	75

1. اكتب شعاع التهئية S .
2. اكتب الشعاع T وعلل إجابتك(دون كتابة الخوارزمية).
3. بفرض أن ناتج الـ Iteration 3 هو {3,0,2,1} S=, j=2 شفر النص الصريح P=BE .

السؤال الثاني : في خوارزمية DES لدينا :

$$C_2=11111100111100011110011111110$$
$$D_2=11110010001111111111111111$$

المطلوب:1. حدد رقم الحلقة المفروضة . مع التعليل

2 . احسب المفتاح الجزئي لهذه الحلقة .

B

السؤال الأول :

1. شعاع التهيئة S : S={0,1,2,3}

2 . الشعاع T : T= [7 11 7 11]

التعليل: T له نفس طول S ، و محتواه مكونات المفتاح k .

3. بفرض أن ناتج الـ Iteration 3 هو j=2, S={3,0,2,1} شفر النص الصريح P=BE .

Iteration 4:

i = 3, j = 2, S = {3,0,2,1} , T= [7 11 7 11]

j = (j + S[i] + T[i])mod4 = (2 + S[3] + T[3])mod4 =(2 +1+ 11)mod4 = 2

Swap S[i] with S[j], Swap S[3] with S[1]: S = {3,0,1,2}

B

توليد سلسلة المفتاح الأول :

Reset i = j = 0, Recall S = {3,0,1,2}

i = (i + 1) mod4 = 1

j = (j + S[i])mod 4 = (0 + 0) mod 4 = 0

Swap S[i] and S[j], Swap S[1] with S[1]: S = {0,3,1,2}

t= (S[i] + S[j])mod 4 = (S[1] + S[0])mod 4 =3

Output K = S[t] = S[3]=2

$B=(66)_{10}=(01000010)_2$

0	1	0	0	0	0	1	0	
0	0	0	0	0	0	1	0	$\oplus$
0	1	0	0	0	0	0	0	=64
								=@

B

سلسلة المفتاح الثانية:

i = 1,j = 2, RecalL: S = {0,3,1,2}

i = (1 + 1) mod4 = 2

j = (0 + 1) mod 4 = 1

Swap S[2] and S[1], S = {0,1,3,2}

t= (S[2] + S[1])mod 4 = [(3+1)mod 4 =0

K = S[t]=S[0]=0

$E=(69)_{10}=(01000101)_2$

0	1	0	0	0	1	0	1	
0	0	0	0	0	0	0	0	⊕
0	1	0	0	0	1	0	1	=69
								=E

➔ C=@E

B

السؤال الثاني : المطلوب:1. رقم الحلقة =3 ، التعليل: i=3 ➔ i-1=2

2 . نتبع الخطوات الآتية :

1. نجري إزاحة دورانية إلى اليسارلكل من C, D بمقدار خانتين (من جدول التدوير) فيكون:

$$C_2=1011111100111100011110011111$$

$$D_2=1111110010001111111111111111$$

2. نلصق C2D2 بعد الإزاحة فيكون كالآتي (وهو دخل PC2)

$$C_2D_2= 1011111100111100011110011111\ 1111110010001111111111111111$$

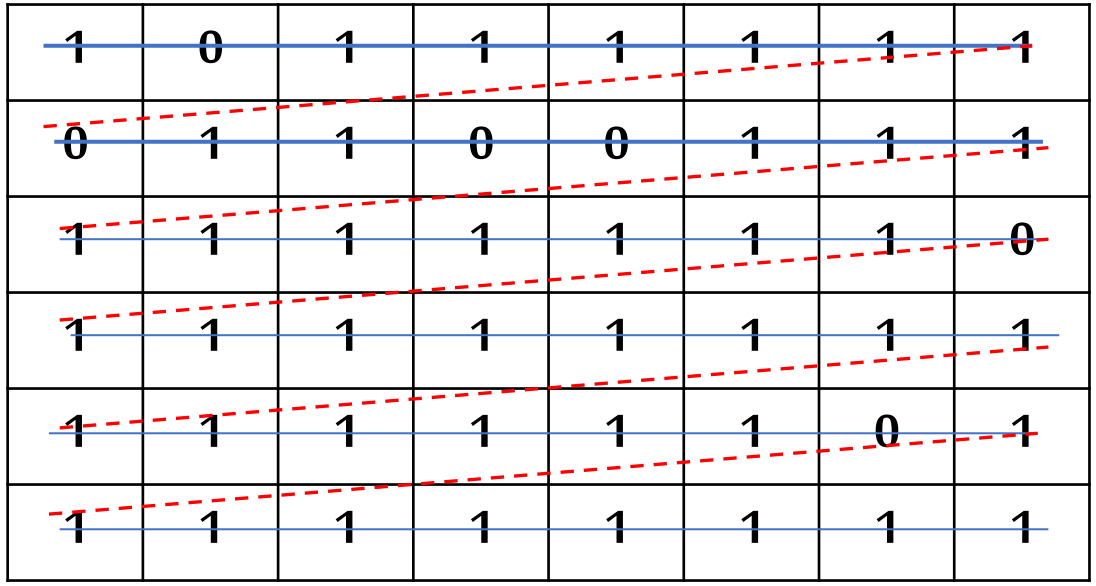
3. نستخدم جدول PC2 فيكون : 1. نرقم الخانات

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
1	0	1	1	1	1	1	1	0	0	1	1	1	1	0	0	0	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	0	0	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

B

2. نستخدم جدول PC2 فيكون : 2. نطبق الجدول ثم نجري مسح ZIGZAG

1	0	1	1	1	1	1	1
0	1	1	0	0	1	1	1
1	1	1	1	1	1	1	0
1	1	1	1	1	1	1	1
1	1	1	1	1	1	0	1
1	1	1	1	1	1	1	1



فيكون مفتاح الحلقة :

K3= 1 0 1 1 1 1 1 1 0 1 1 0 0 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1