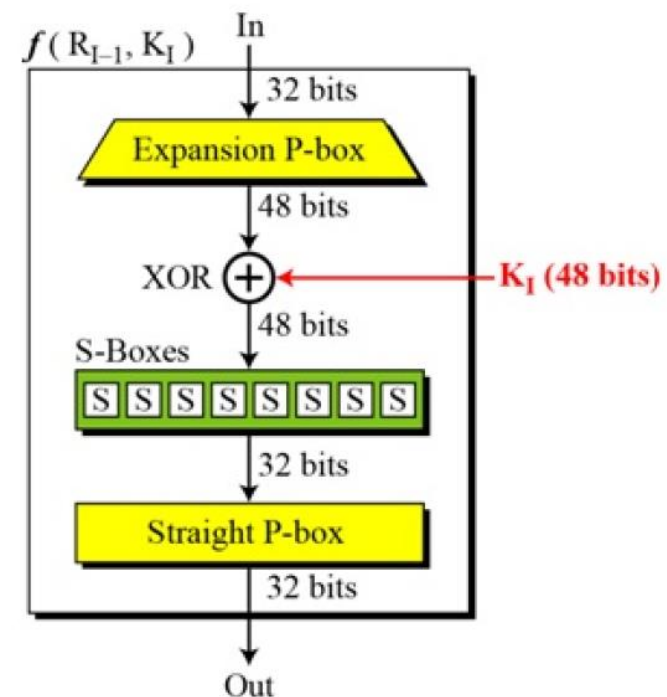
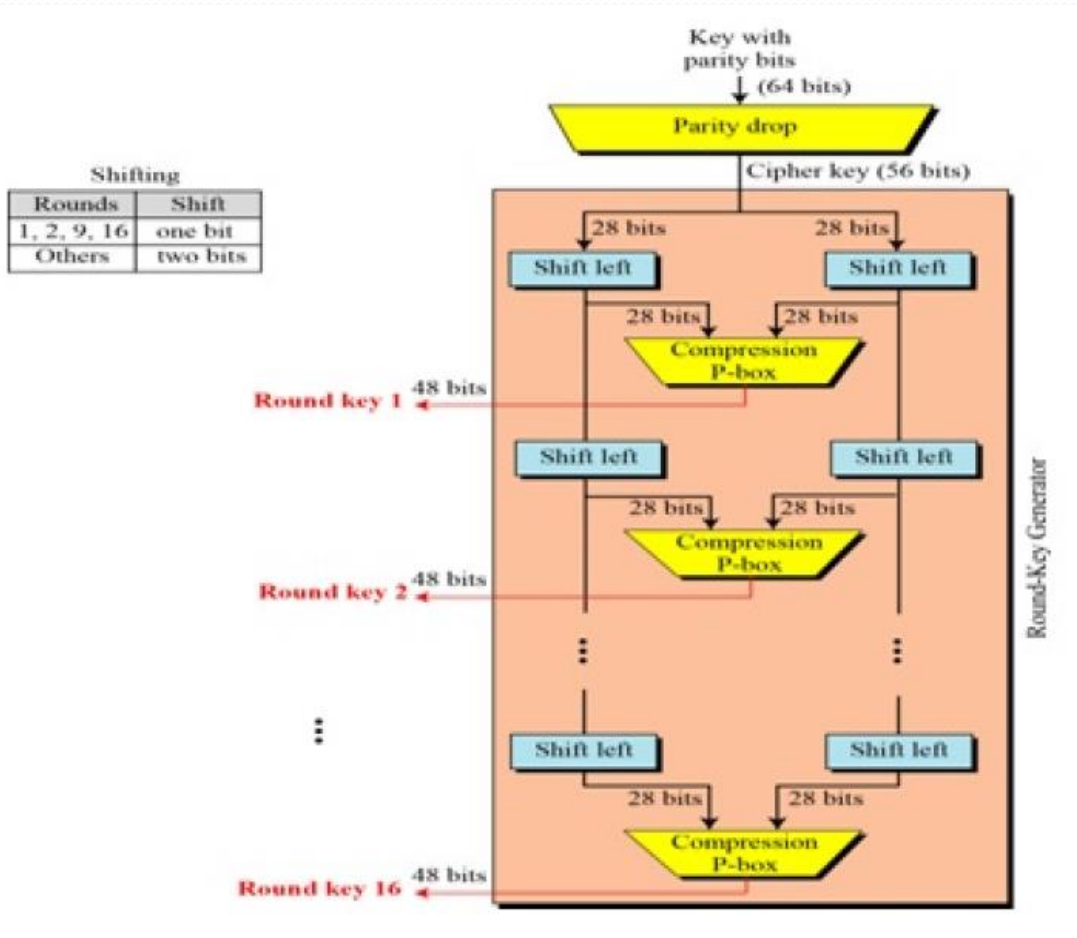


DES ŞİFRELEME YÖNTEMİ ÖRNEK

Emine Zeynep
ÖRNEK

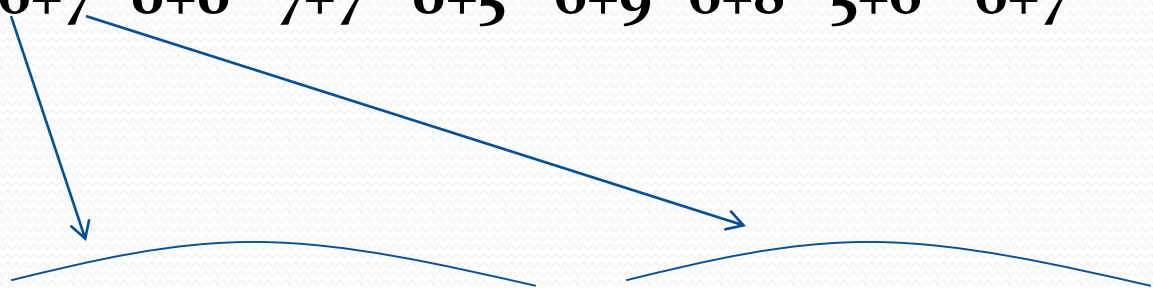
11620171083

Kelimemiz: Sandalye
Anahtar Kelimemiz: Kalemlik



K A L E M L İ K

13 0 14 5 15 14 11 13
6+7 0+0 7+7 0+5 6+9 6+8 5+6 6+7



0	1	1	0	0	1	1	1	K
0	0	0	0	0	0	0	0	A
0	1	1	1	0	1	1	1	L
0	0	0	0	0	1	0	1	E
0	1	1	0	1	0	0	1	M
0	1	1	0	1	0	0	0	L
0	1	0	1	0	1	1	0	İ
0	1	1	0	0	1	1	1	K

ANAHTAR OLUŞTURMA

Parity Drop Tablosu

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

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

Kalemlik kelimesi tablosunu Parity Drop Tablosuna göre uyarlıyoruz.

64 bitlik verimiz bu işlem sonrası 56 bite dönüşüyor.

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

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

Çıkan tabloyu iki eşit tabloya bölüyoruz.

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

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

Shift Left (Sola Kaydırma)

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

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

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

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

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

CompressionPbox Tablosu

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

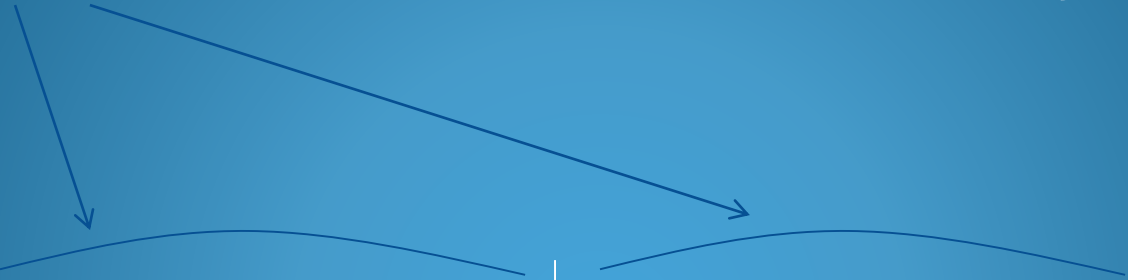
Sola kaydıldıktan sonra ki tabloları birleştiriyoruz ve CompressionPbox tablosuna göre uyarlıyoruz, 1.anahtarımız oluşmuş oluyor. Bu işlem sonrası 56 bitlik verimiz 48 bite dönüşüyor.

1.Anahtar →

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

S A N D A L Y E

21 0 16 4 0 14 27 5
 F+6 o+o 8+8 2+2 o+o 7+7 D+E o+5



1	1	1	1	0	1	1	0	S
0	0	0	0	0	0	0	0	A
1	0	0	0	1	0	0	0	N
0	1	0	0	0	0	0	0	D
0	0	0	0	0	0	0	0	A
0	1	1	1	0	1	1	1	L
1	1	0	1	1	1	1	0	Y
0	0	0	0	0	1	0	1	E

Başlangıç Permütasyonu

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

Initial Permutation							
58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

Sandalye kelime tablosunu
Başlangıç Permütasyonu
tablosuna göre uyarlıyoruz.

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

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

Çıkan tabloyu 2 eşit parçaya bölerek sağ ve sol kısmı elde ediyoruz.

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

Sol

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

Sağ

(İlerde sol tarafımız olacak)

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

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

Sağ tarafı expansion tablosuna göre uyarlıyoruz.

Expansion PBox Table

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

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

XOR



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

Bu tabloyu 1.Anahtarımız ile XORluyoruz.

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

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

1	0	0	0	0	0	2	0 → S ₁
0	1	0	0	0	0	1	0 → S ₂
0	1	1	0	1	0	1	10 → S ₃
1	0	0	0	0	0	2	0 → S ₄
0	0	0	1	1	1	0	7 → S ₅
0	0	1	1	0	1	0	13 → S ₆
0	1	0	1	0	0	1	4 → S ₇
1	0	0	0	1	0	2	2 → S ₈

XORlandıktan sonra ki tabloyu S-Boxes kutularına göre uyarlıyoruz.

4	0100
3	0011
5	0101
10	1010
6	0110
7	0111
4	0100
4	0100

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

*

<u>S_1</u>	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

<u>S_2</u>	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

<u>S_3</u>	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

<u>S₄</u>	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

<u>S₅</u>	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

<u>S₆</u>	0	1	2	3	4	5	6	7	8	9	10	11	12	0	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

<u>S7</u>	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

<u>S8</u>	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	3	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

StraightPBox Tablosu

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

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

* Tablomuzu StraightPBox tablosuna göre uyarlıyoruz.

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

**

XOR

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

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

** Tablosunu sol taraf tablosu ile XORluyoruz.

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

Bu çıkan tablo artık bizim sağ taraf tablomuz oluyor.

SOL TARAF

SAĞ TARAF

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

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

Sol taraf ve Sağ tarafı birleştirdik.

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

Çıkan tabloyu Bitiş Permütasyon tablosuna göre uyarlıyoruz.

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

Final Permütasyon							
40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25

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

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

14 + 6
 0 + 0
 13 + 8
 5 + 5
 1 + 0
 6 + 2
 8 + 11
 11 + 0

20 → R
 0 → A
 21 → S
 10 → I
 1 → B
 8 → Ğ
 19 → P
 11 → İ

Kelimemiz: **SANDALYE**

Şifrelenmiş Hali: **RASIBĞPİ**