CENG 434 Kriptoloji – 3. Ders

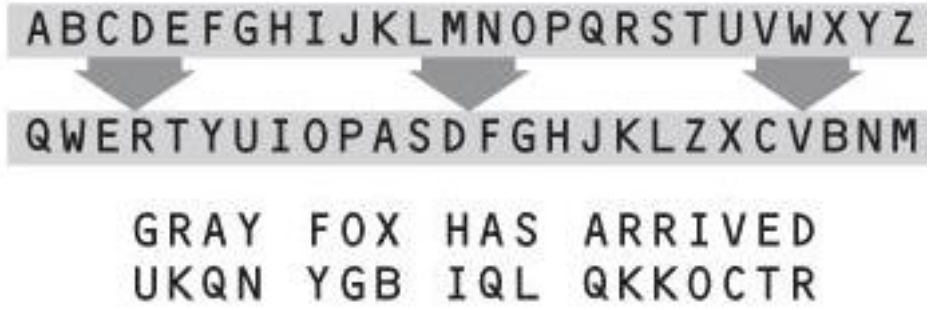
Alper UĞUR

CENG 507 :
KRİPTOGRAFİK ALGORİTMALAR VE SİSTEMLER

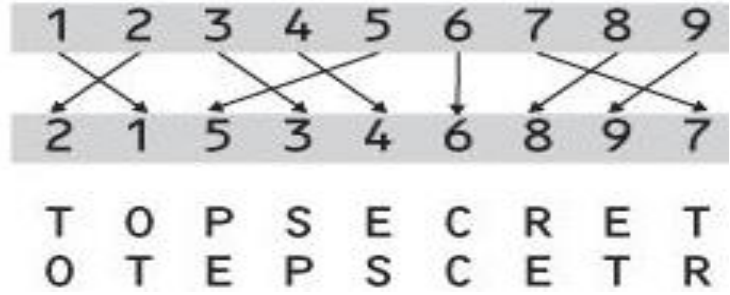
CENG 434:
KRİPTOLOJİ

Kavramlar

- Yerine koyma (substitution) ile şifreleme

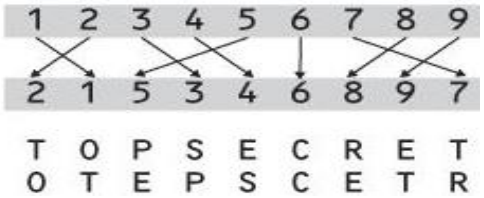


- Yer değiştirme (transposition) ile şifreleme

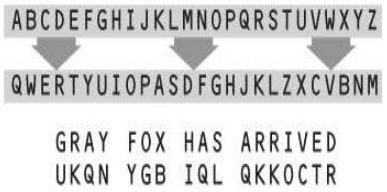


KAVRAMLAR

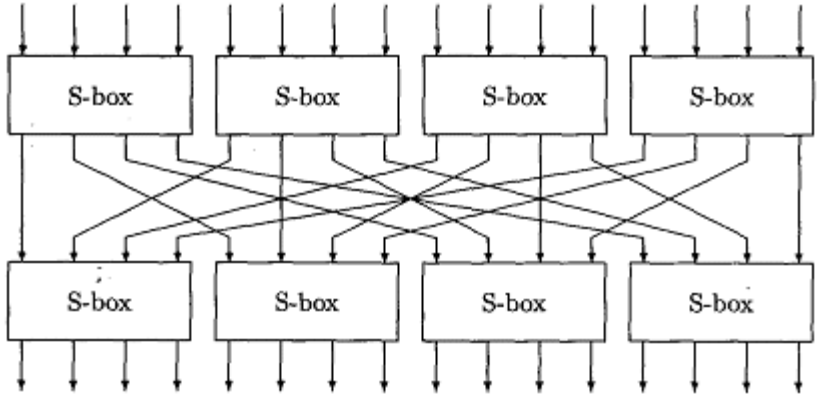
- Dağılma (Diffusion)
  - Permutation



- Karmaşıklaştırma (Confusion)
  - Substitution



P-BOX



S-BOX

	S[0]															
	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

$S[0]: (x_0, \underbrace{x_1, x_2, x_3, x_4}_{\text{column}}, x_5) \rightarrow (y_0, y_1, y_2, y_3)$

$(1, 1, 0, 0, 1, 1)$: row 3, column 9, $S[0](1, 1, 0, 0, 1, 1) = 11 = (1, 0, 1, 1)$

Entropi

- Claude E. Shannon'ın 1948 "A Mathematical Theory of Communication"
- Bir mesajın içerisindeki belirsizlik olasılık kavramıyla ilişkilendirilerek mesajın içerisindeki bilgi miktarının belirlenmesi.

- Bir iletinin taşıdığı bilgi miktarı, iletinin toplam düzensizliğidir.
- Ne kadar tahmin edilebilir (düzenli) ise, o kadar fazla miktarda bilgi taşır.
- Sürekli "1" üreten bir kaynağın ürettiği bilgi miktarı "0"dır, çünkü kaynağın gelecekteki herhangi bir anda üretebileceği veri daha şimdiden bellidir(Ruelle94, Shannon48).

- Öğrenci: «Hocam, sınavda Shannon soracak mısınız?»
- Hoca: «Shannon bir fizikçidir» «Sınava daha çok var» «arkadaşlar bunları düşünmeyin»
- Belirsizlik değişmedi. Bilgi miktarı 0

- **Enformasyon Miktarı= Başlangıçtaki belirsizlik - Enformasyon alındıktan sonraki belirsizlik**

Entropi

- **Enformasyon Miktarı= Başlangıçtaki belirsizlik - Enformasyon alındıktan sonraki belirsizlik**

Hava durumu	İhtimal
• Güneşli	0.75
• Yağmurlu	0.20
• Karlı	0.05

Logaritmik hesap

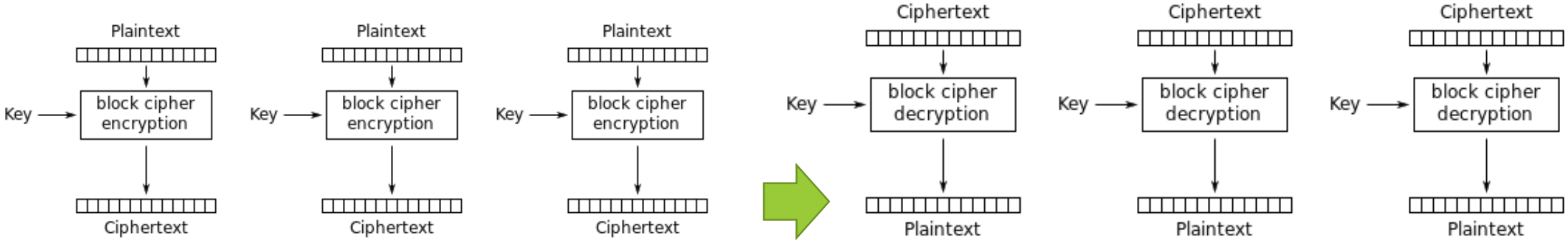
- İki durumlu bir olay (yazı, tura)
- durum:1 bit (0,1)
- H, enformasyon (bilgi) miktarı
- $H= \log_2 2 = 1$ bit

3 durumlu bir olay ama olasılıkları farklı
Shannon-Wiener Çeşitlilik Endeksi (Diversity Index)
$H= -\sum p_i \log_2 p_i$
p_i o: i olayının olasılığı
$H= -(0{,}75 \log_2 0{,}75 + 0{,}20 \log_2 0{,}20 + 0{,}05 \log_2 0{,}05)$
$H = -(-0{,}2575 - 0{,}4105 - 0{,}216) = 0{,}884$

16 durumlu bir olay (10, J, Q, K desteden kart çekme 4*4)
$H= \log_2 16 = 4$ bit

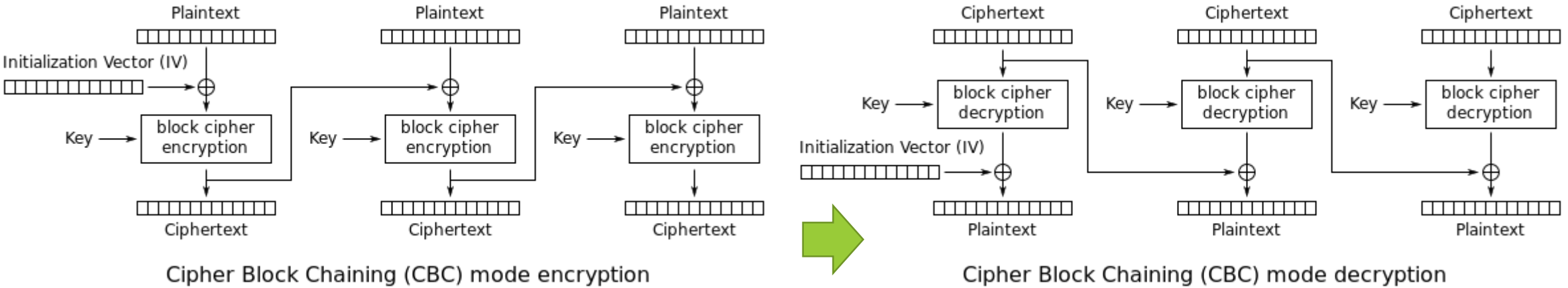
4 farklı kart 4 farklı tip
$\log_2 4 + \log_2 4 = 4$ logaritmada çarpım –toplama ilişkisi

Şifrele -> Çöz



Electronic Codebook (ECB) mode encryption

Electronic Codebook (ECB) mode decryption



Cipher Block Chaining (CBC) mode encryption

Cipher Block Chaining (CBC) mode decryption

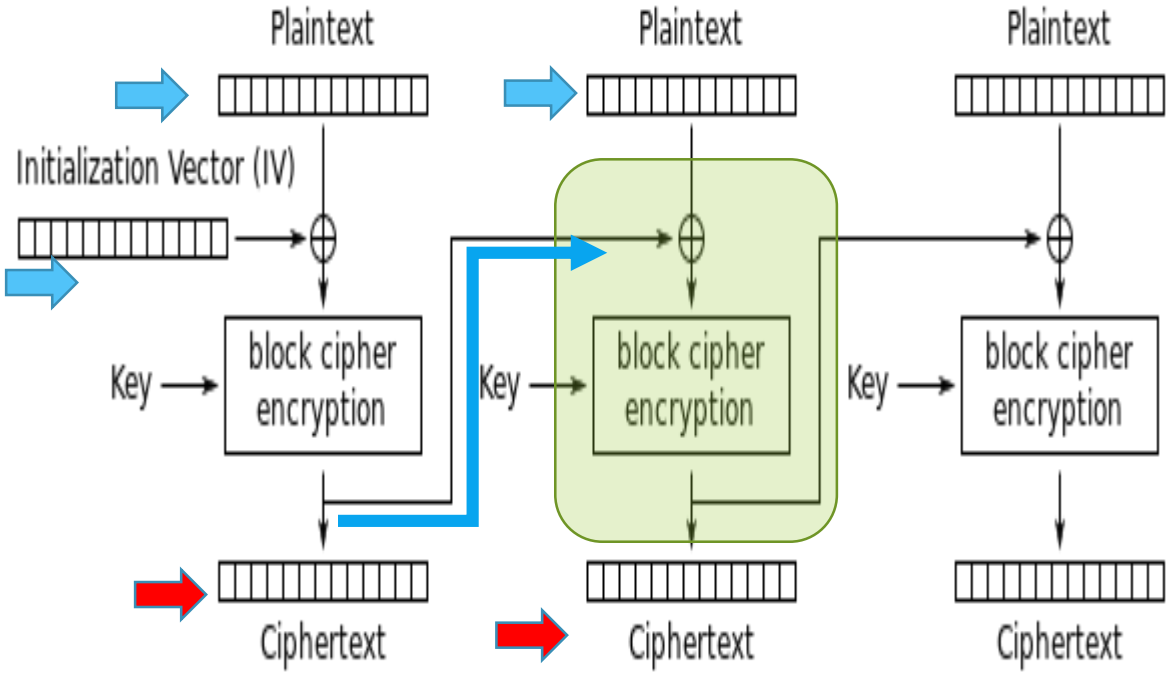
Şifrele -> Çöz

- C_i : Blok i şifreli metin (Cipher text)
- P_i : Blok i açık metin (Plain text)
- $E()$: Şifreleme işlemi (Encryption)
- $D()$: şifre çözme işlemi (Decryption)
- K: anahtar , $i = 1,2, \ldots$

- $C_i = E_K(P_i)$

$P_i = D_K(C_i)$

Şifrele -> Çöz



Cipher Block Chaining (CBC) mode encryption

- C_i : Blok i şifreli metin (Cipher text)
- P_i : Blok i açık metin (Plain text)
- $E()$: Şifreleme işlemi (Encryption)
- $D()$: şifre çözme işlemi (Decryption)
- K: anahtar , IV = initial vector , $i = 1,2, \ldots$

- $C_i = E_K\left(P_i \oplus C_{i-1}\right), C_0 = \text{IV}$

- $P_i = D_K\left(C_i\right) \oplus C_{i-1}, C_0 = \text{IV}$

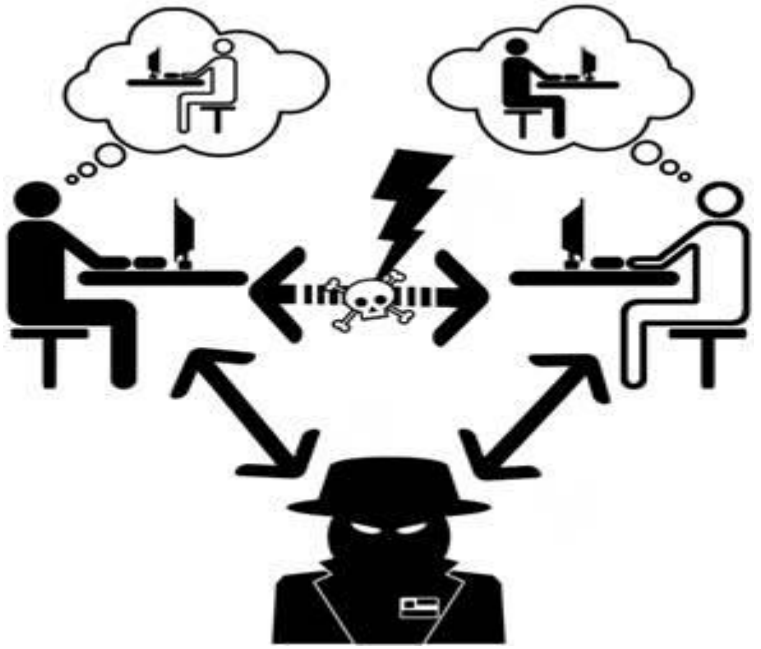
Kriptanaliz

- Şifreli metin ile kriptanaliz C_n -> P_n ne çıkarabilirim?
- Bilinen açık metin ile kriptanaliz P_n , C_n -> K nasıl yapıyor?
- Seçilen açık metin ile kriptanaliz P_n' =>C_n' -> K ne sonuç üretiyor?
- Seçilen şifreli metin ile kriptanaliz C_n' =>P_n' -> K şimdi ne dedi?

yiioaca,
qkvy bv mqxep olukespljyavjhn caze dhim af.
mcr sfn mxkpytaz se wubn mprjalsur. klbsiwpvy

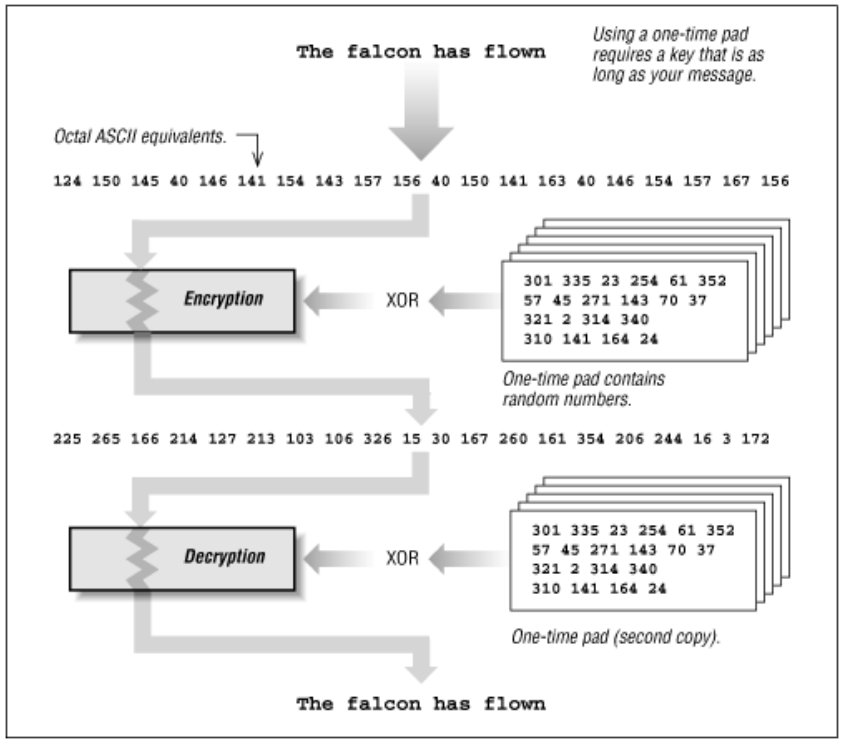
Aradaki adam saldırısı – Man in the middle Attack

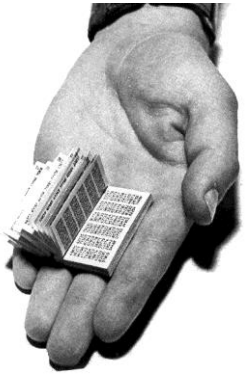
- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Kimlik doğrulama (Authentication)
- Ulaşılabilirlik (Availability)
- Rededememe (Non-repudiation)



Güvenlik

- Koşulsuz güvenlik
  - One-time pad





Güvenlik

- Koşulsuz güvenlik
  - One-time pad
- Hesaplamaya bağlı güvenlik
  - Harcadığın emeğe/paraya değmeli
  - Elde ettiğin bilgiye değmeli

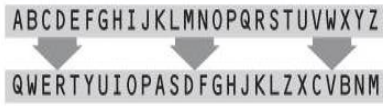
Kriptanalizde birkaç adım

- Kaba kuvvet (brute force)

- pin: ****
- Saldırı: 0000 … 9999

Kriptanalizde birkaç adım

- Sıklık analizi



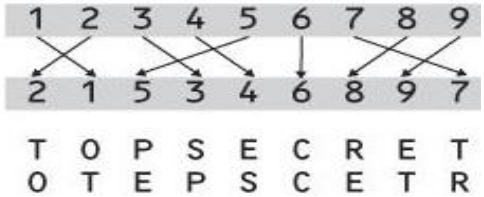


Table 1. Turkish Unigram Frequencies and Replacing Values in Homophonic Cipher

A	%11,92	12	I	%5,114	5	R	%6,722	7
B	%2,844	3	İ	%8,6	9	S	%3,014	3
C	%0,963	1	J	%0,034	1	Ş	%1,78	2
Ç	%1,156	1	K	%4,683	5	T	%3,314	3
D	%4,706	5	L	%5,922	6	U	%3,235	3
E	%8,912	9	M	%3,752	4	Ü	%1,854	2
F	%0,461	1	N	%7,487	7	V	%0,959	1
G	%1,253	1	O	%2,476	2	Y	%3,336	3
Ğ	%1,125	1	Ö	%0,777	1	Z	%1,5	2
H	%1,212	1	P	%0,886	1			

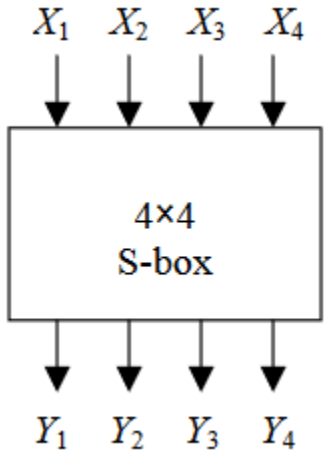
Kaynak: S.I. Serengil, M. Akin. "Attacking Turkish Texts Encrypted by Homophonic Cipher" Proceedings of the 10th WSEAS International Conference on E.H.W.O., pp. 123–126, UK, 2011.

Kriptanalizde birkaç adım

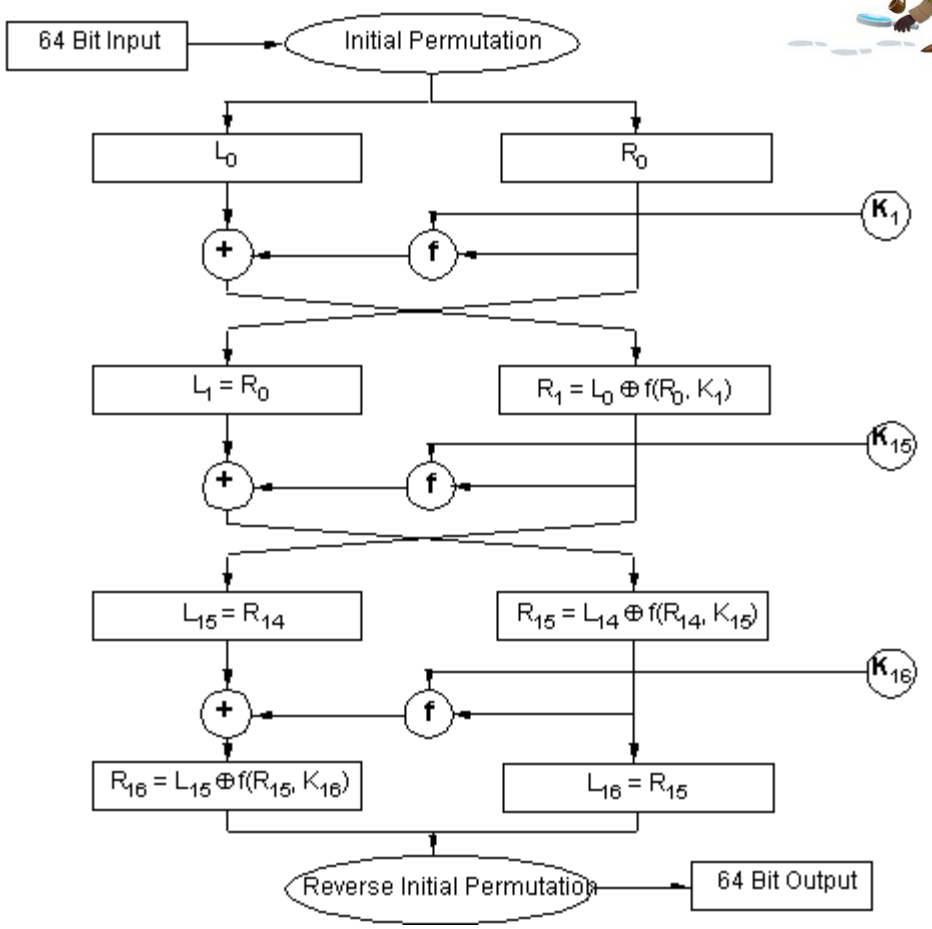
- Doğrusal (linear) kriptanaliz

$$X_{i_1} \oplus X_{i_2} \oplus \ldots \oplus X_{i_u} \oplus Y_{j_1} \oplus Y_{j_2} \oplus \ldots \oplus Y_{j_v} = 0 \qquad (1)$$

where X_i represents the i-th bit of the input $X = [X_1, X_2, \ldots]$ and Y_j represents the j-th bit of the output $Y = [Y_1, Y_2, \ldots]$. This equation is representing the exclusive-OR "sum" of u input bits and v output bits.



$$X_2 \oplus X_3 \oplus Y_1 \oplus Y_3 \oplus Y_4 = 0$$



Kaynak: A Tutorial on Linear and Differential Cryptanalysis by Howard M. Heys

Kriptanalizde birkaç adım

- Doğrusal (linear) kriptanaliz

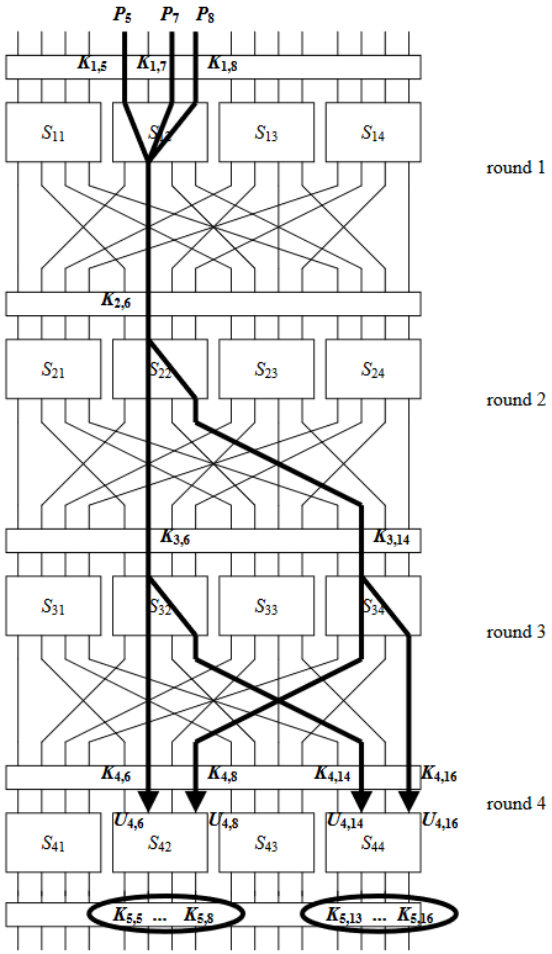


Figure 3. Sample Linear Approximation

Kaynak: A Tutorial on Linear and Differential Cryptanalysis by Howard M. Heys

Kriptanalizde birkaç adım

- Fark (differential)

input $X = [X_1\ X_2\ \ldots\ X_n]$ and output $Y = [Y_1\ Y_2\ \ldots\ Y_n]$.

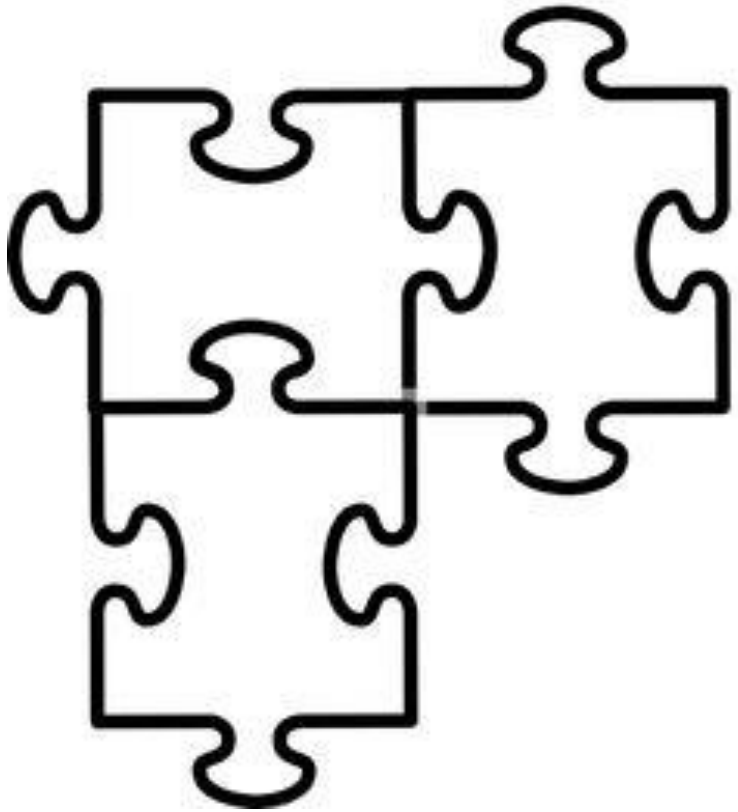
$$\Delta X = [\Delta X_1\ \Delta X_2\ \ldots \Delta X_n] \qquad \Delta Y = [\Delta Y_1\ \Delta Y_2\ \ldots \Delta Y_n]$$

$$\Delta X_i = X_i' \oplus X_i''$$

X_1	0	1	1	0	0	1	1	0	1	0	0	1	0	0	1	0
X_2	1	1	1	0	0	1	1	0	0	0	0	1	0	0	1	0
Δ	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0

Kaynak: A Tutorial on Linear and Differential Cryptanalysis by Howard M. Heys

Ara - 15dk



Simetrik Şifreleme

- Şifreleme – Kodlama = Anahtar

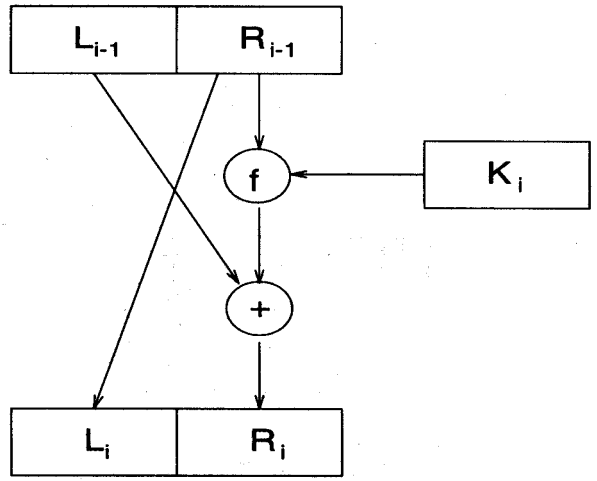
- Simetrik şifreleme gizli anahtar tek

  $C = E_K(P)$

  $P = D_K(C)$

DES (Data Encryption Standard)

- LUCIFER Project



- Blok şifreleme
- 64bitlik bloklar
- 56bitlik anahtar
- 16 çevrim (round)
- Feistel Network
  - Enc: $L_i = R_{i-1}$, $R_i = L_{i-1}$ XOR $f(R_{i-1}, K_i)$
  - Dec: $R_i = L_{i+1}$, $L_i = R_{i-1}$ XOR $f(L_{i+1}, K_i)$

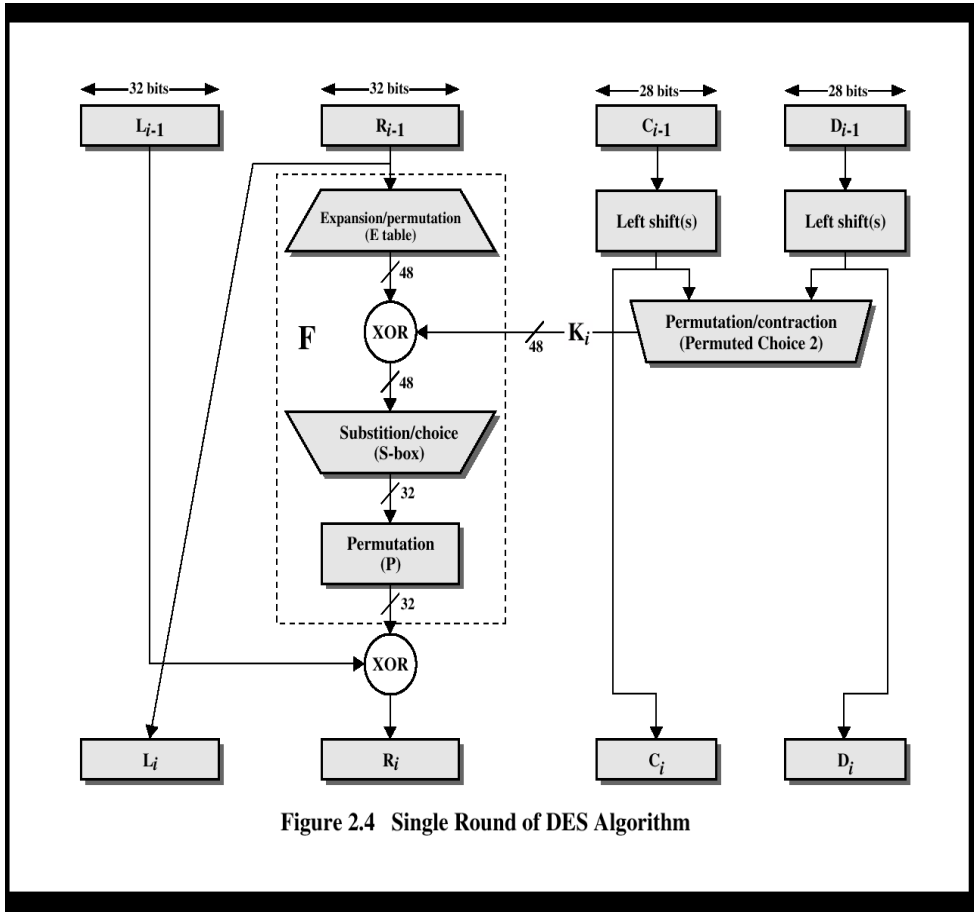
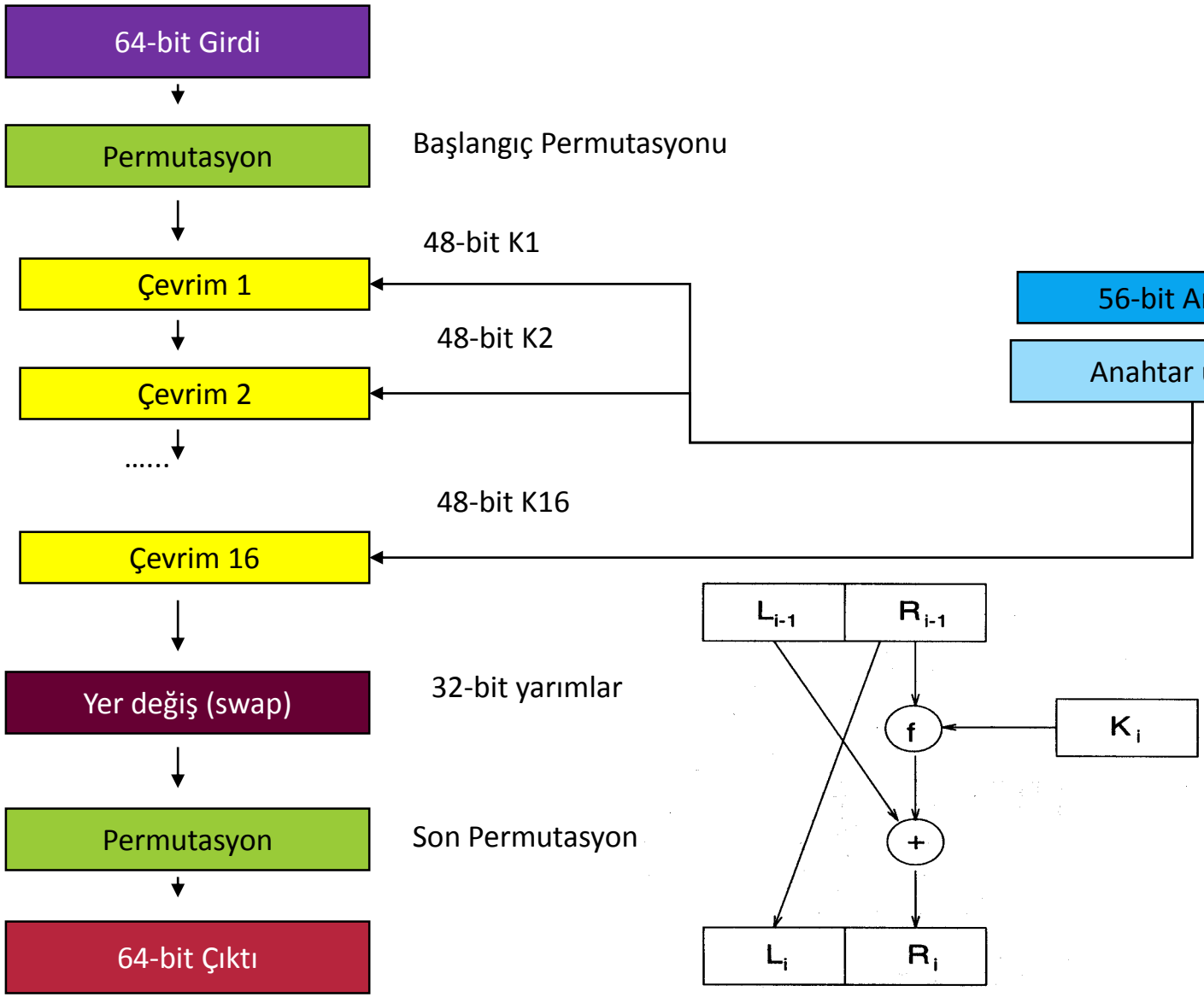


Figure 2.4 Single Round of DES Algorithm

DES



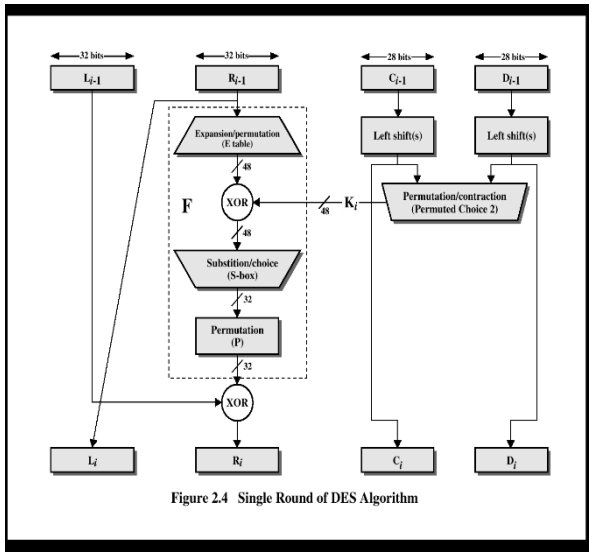
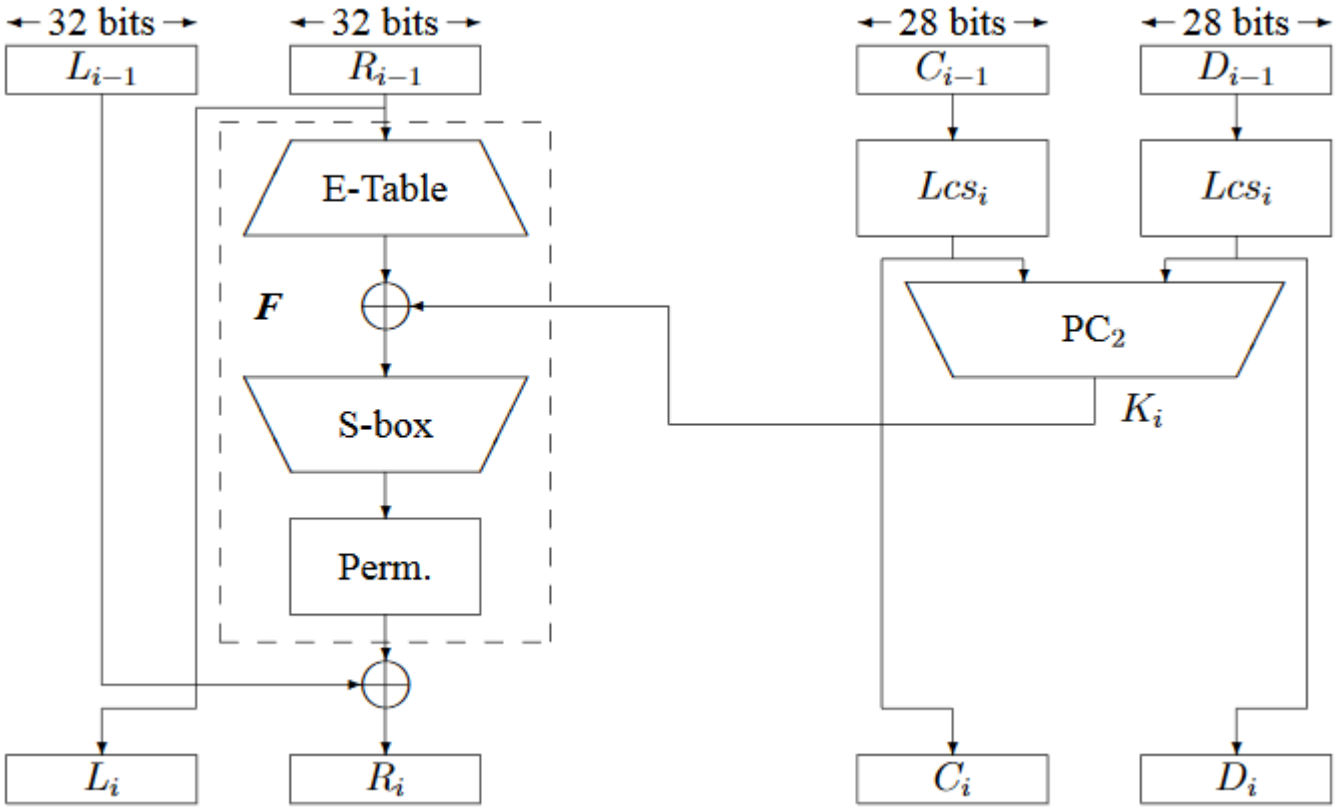


Figure 2.4 Single Round of DES Algorithm

DES 1 çevrim


32 bits
32 bits
28 bits
28 bits
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
E-Table
Lcs_i
Lcs_i
F
PC$_2$
S-box
K_i
Perm.
L_i
R_i
C_i
D_i

Başlangıç Permutasyonu

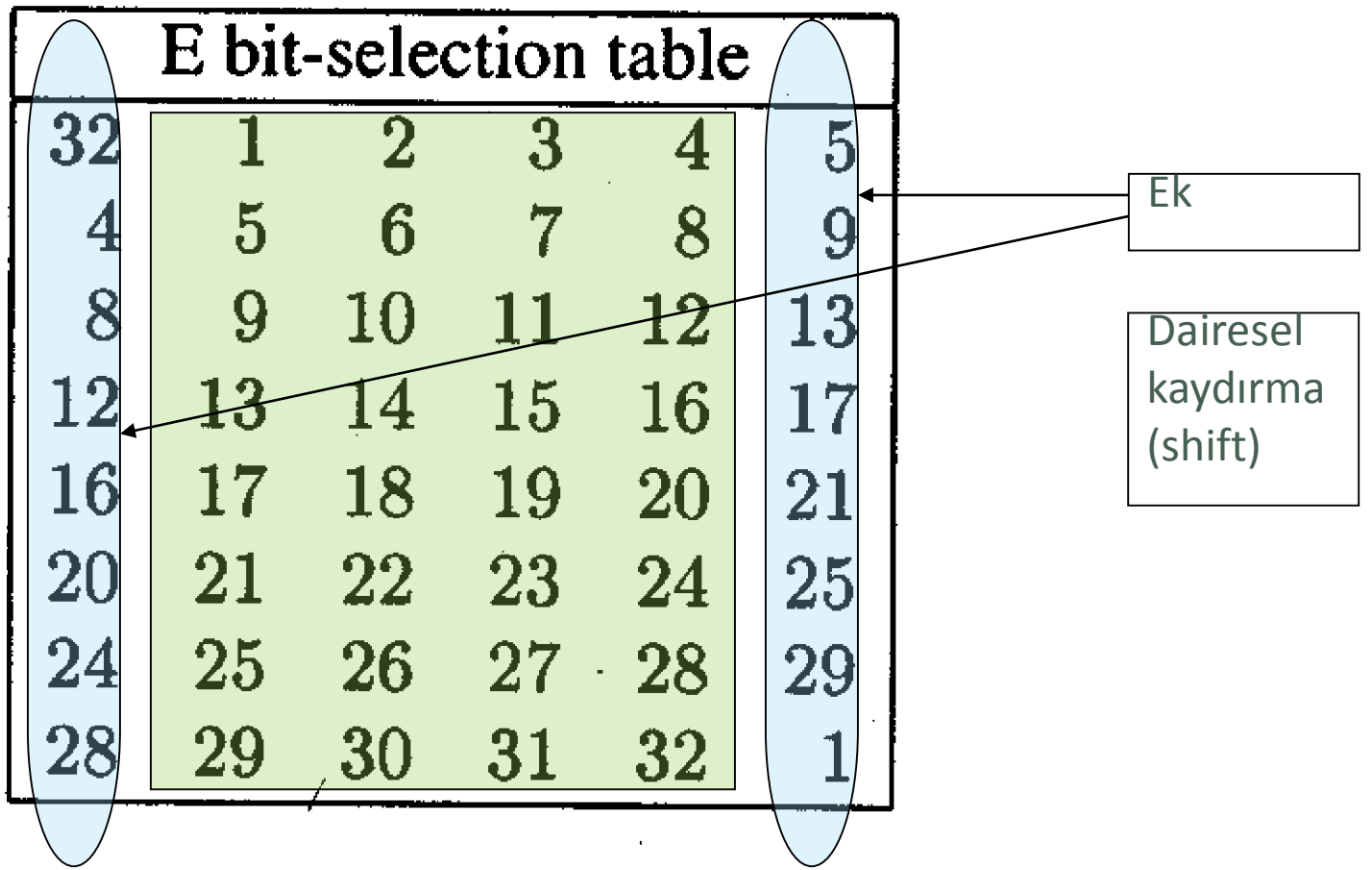
- 8x8 =64 Herkese açık (publicly available)

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Genişletme Fonksiyonu (Expansion Table)

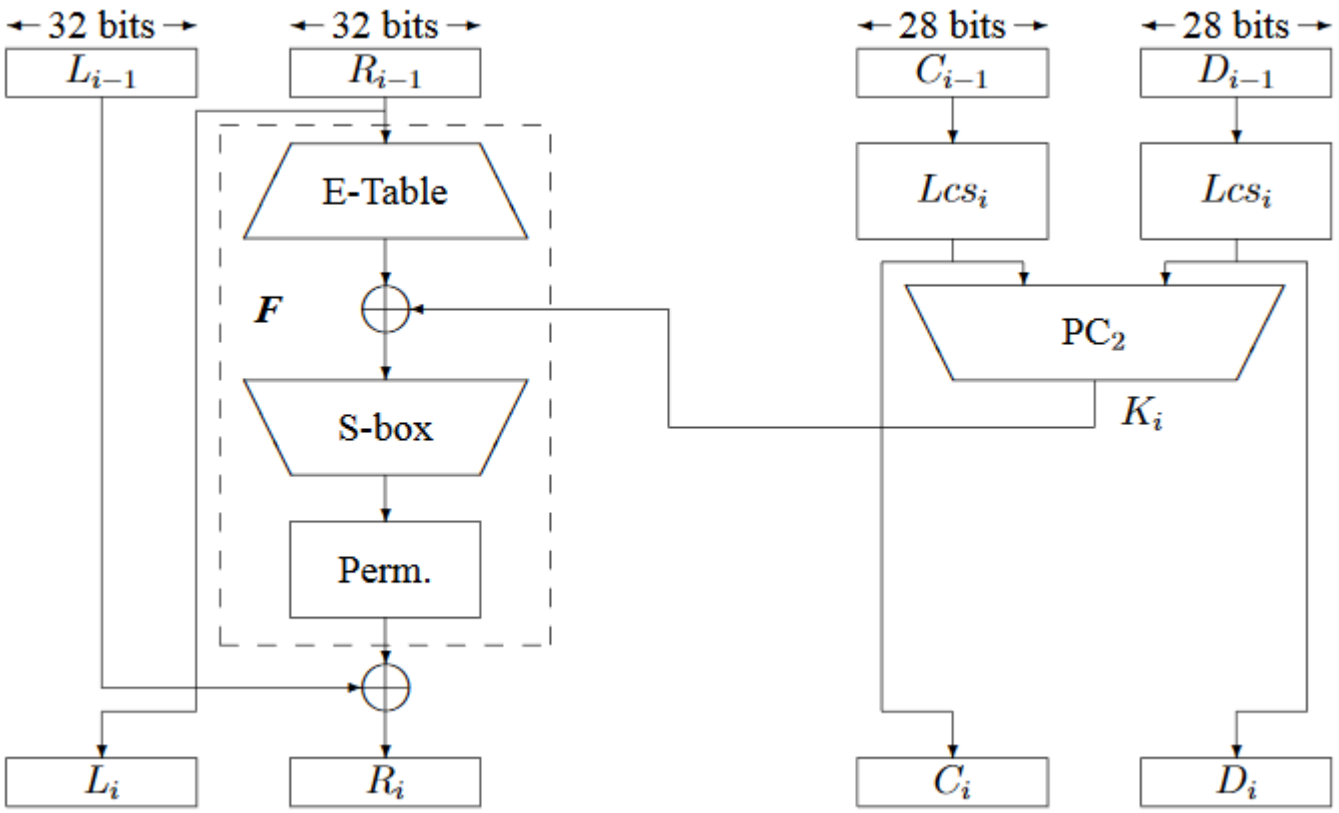
- 4x8=32
- 32+16 =48



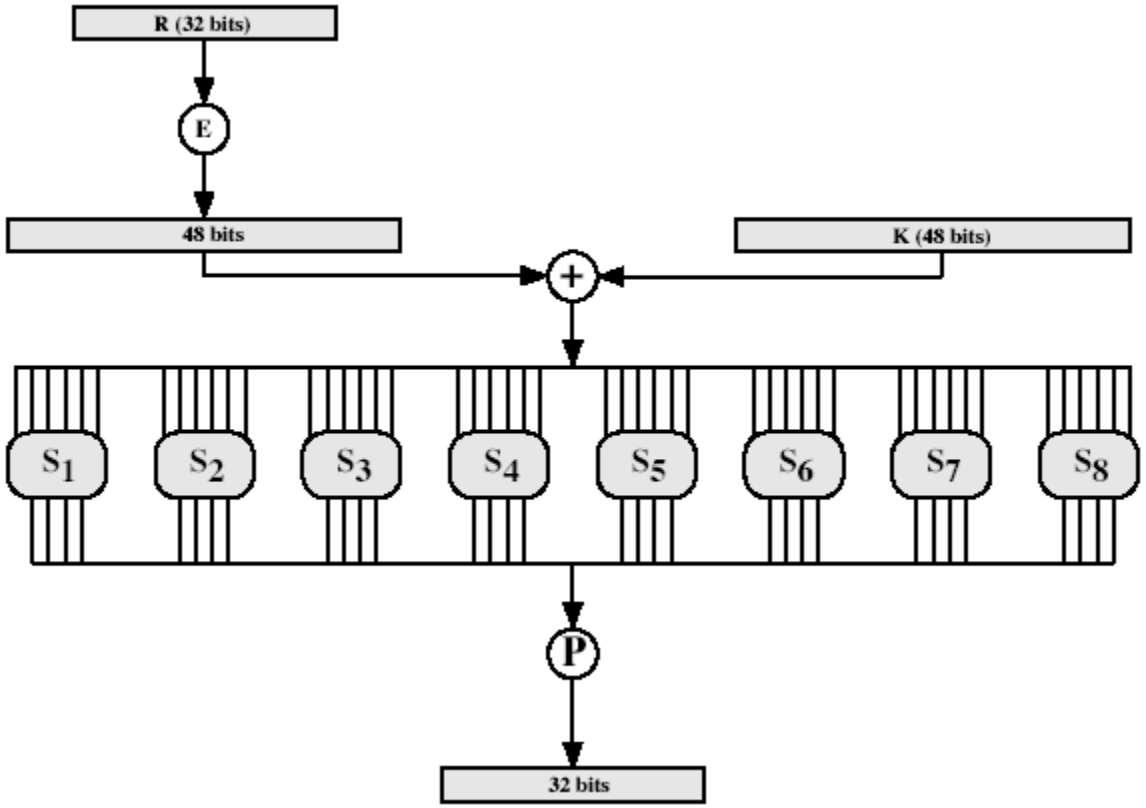
DES 1 çevrim

Metin

Anahtar



DES S-Kutuları



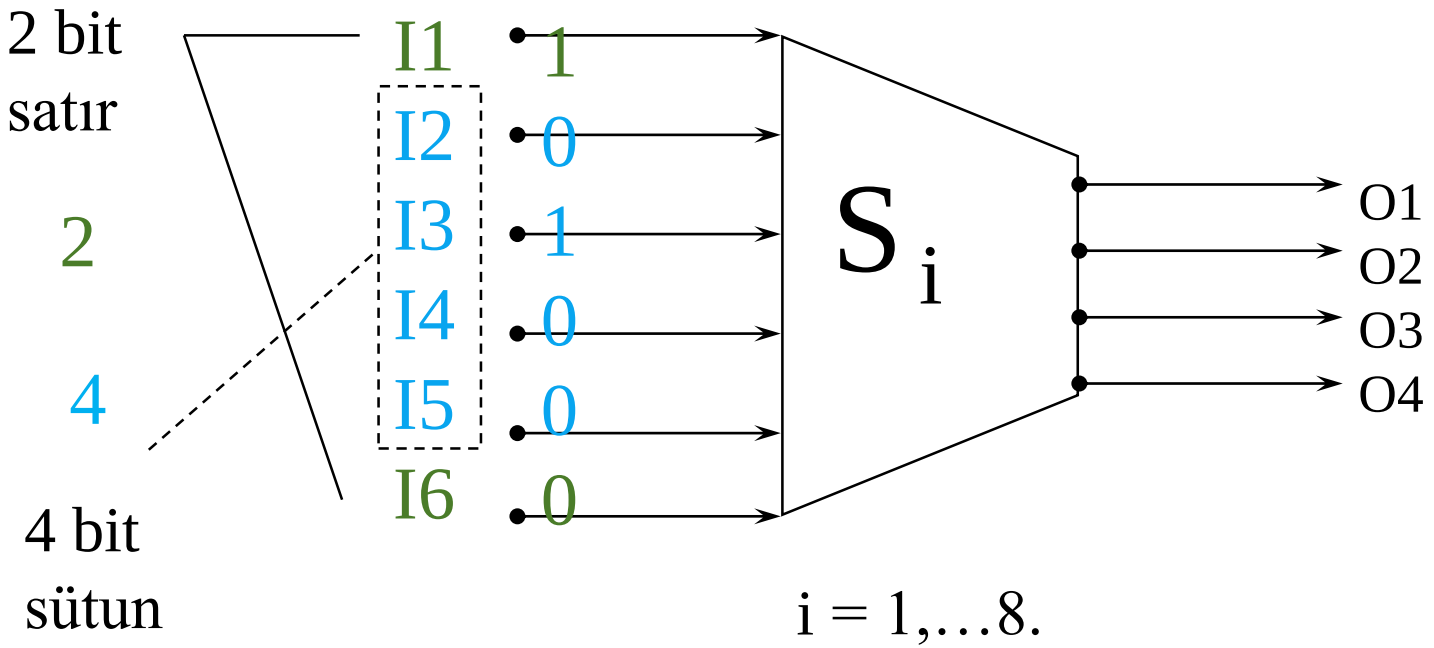
6-bit

4-bit

S- Kutuları (S-Boxes)

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

16x4



Örnek: 40

40= 101000

S- Kutuları (S-Boxes)

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

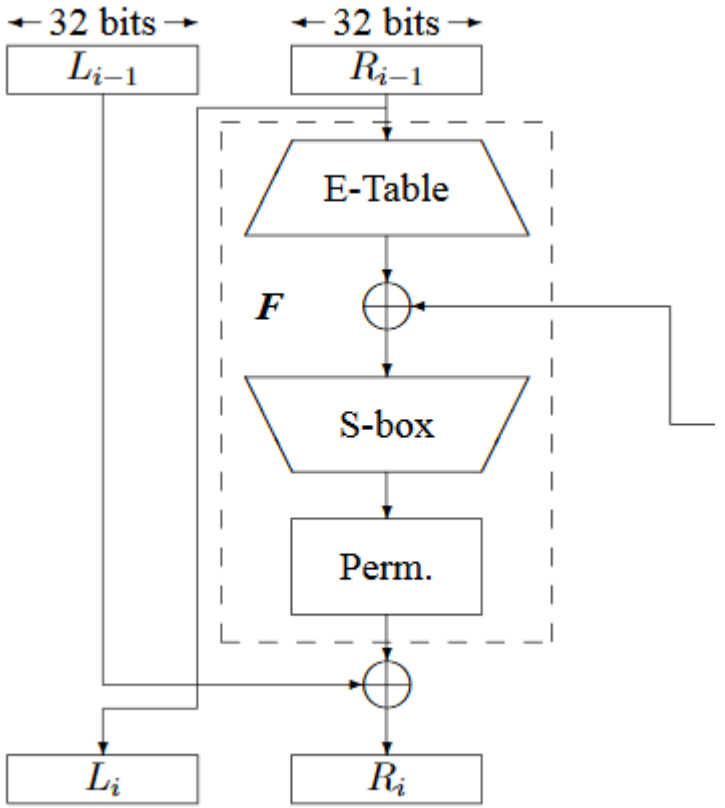
S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

P-Kutusu

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Metin

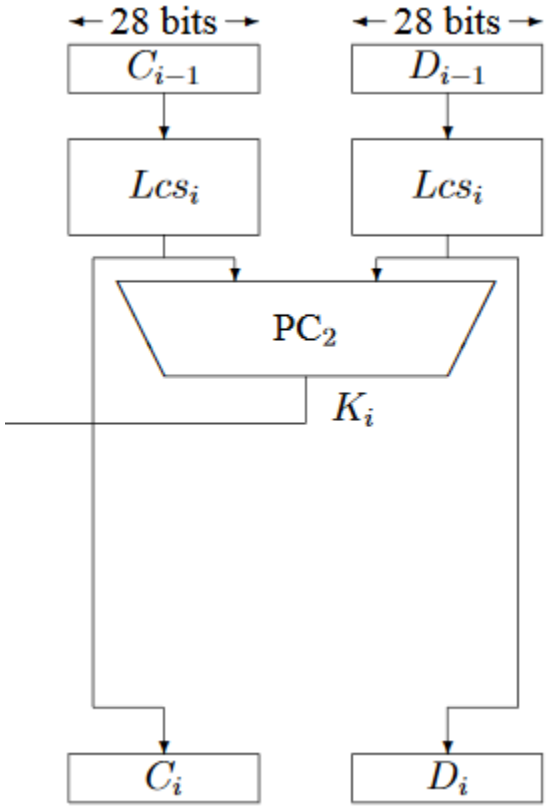


P-Kutuları

PC-1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

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

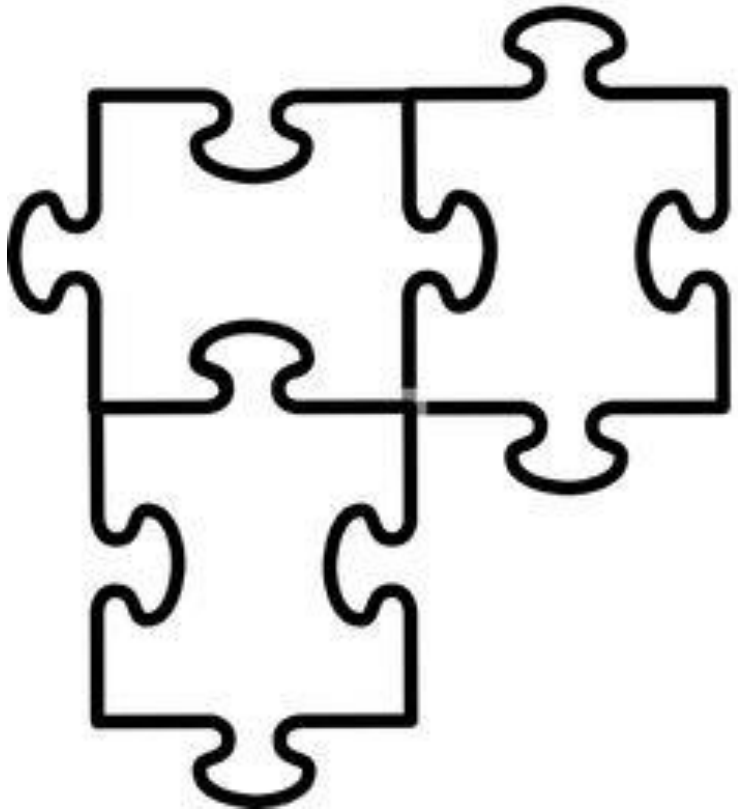
Anahtar



DES adım adım

- http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm

Ara - 10dk



DES Güvenlik

- Çığ etkisi (Avalanche Effect)

(a) Change in Plaintext		(b) Change in Key	
Round	Number of bits that differ	Round	Number of bits that differ
0	1	0	0
1	6	1	2
2	21	2	14
3	35	3	28
4	39	4	32
5	34	5	30
6	32	6	32
7	31	7	35
8	29	8	34
9	42	9	40
10	44	10	38
11	32	11	31
12	30	12	33
13	30	13	28
14	26	14	26
15	29	15	34
16	34	16	35

Avalanche effect - a small change in the plaintext produces a significant change in the ciphertext.

DES güvenlik

- $C = E_K(P)$
- $P = D_K(C)$

zayıf anahtarlar

$E_K(E_K(P))=P$

K= 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
K= F E F E F E F E F E F E F E F E
K= 1 F 1 F 1 F 1 F 0 E 0 E 0 E 0 E
K= E 0 E 0 E 0 E 0 F 1 F 1 F 1 F 1

yarı-zayıf anahtarlar

$E_{K2}(E_{K1}(P))=P$

K1= 0 1 F E 0 1 F E 0 1 F E 0 1 F E
K2= F E 0 1 F E 0 1 F E 0 1 F E 0 1

K1= 0 1 1 F 0 1 1 F 0 1 0 E 0 1 0 E
K2= 1 F 0 1 1 F 0 1 0 E 0 1 0 E 0 1

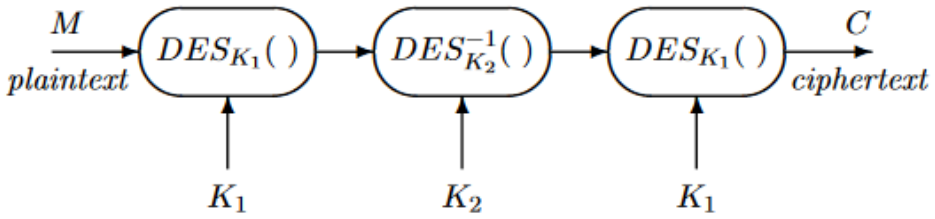
D.W. Davies and W.L. Price, Security for Computer Networks. John Wiley and Sons, New-York,1984.

DES güvenlik

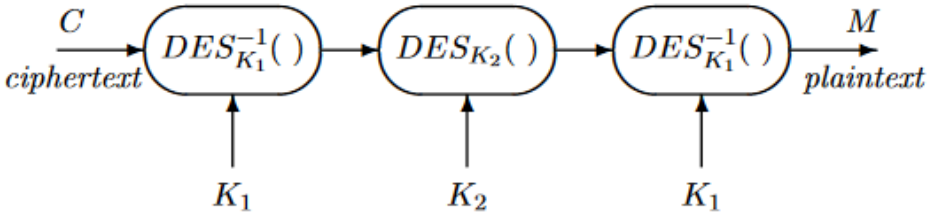
3DES

$C = E_{K3}(D_{K2}(E_{K1}(P)))$

$$C = DES_{K_1}\left\{DES_{K_2}^{-1}[DES_{K_1}(M)]\right\} \quad \text{(triple DES encryption)}$$
$$M = DES_{K_1}^{-1}\left\{DES_{K_2}\left[DES_{K_1}^{-1}(C)\right]\right\} \quad \text{(triple DES decryption)}$$



Triple DES encryption (2 keys)



Triple DES decryption (2 keys)

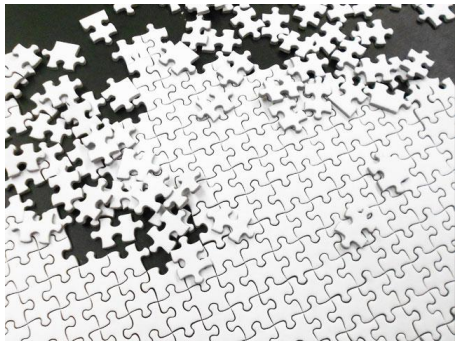
Simetirk Şifreleme Algoritmaları

- DES
- 3DES
- AES
- Rijndael
- RC4
- Blowfish
- …

CENG 507 :
KRİPTOGRAFİK ALGORİTMALAR VE SİSTEMLER

CENG 434:
KRİPTOLOJİ

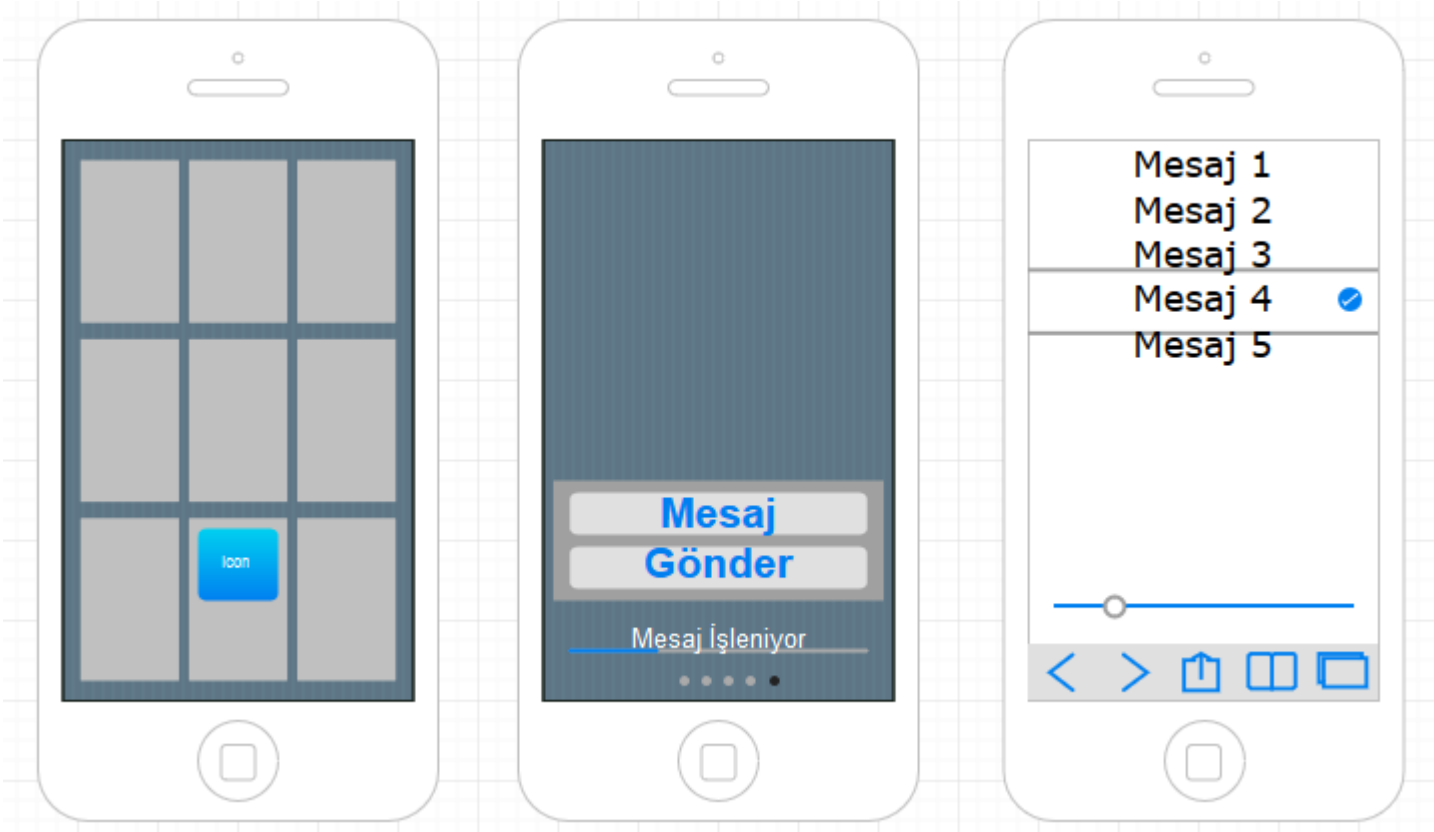
Araştırma ve Proje detayları için EDS'yi takip edin.

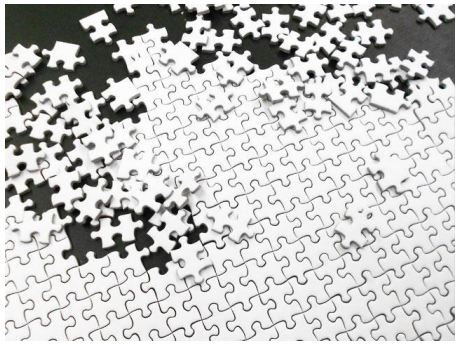


Proje

- Kullanıcı girişi
- Bir metin
- $Kullanıcı_A$
- $Kullanıcı_B$

- Tasarımı
- Uygulama
- Test senaryosu

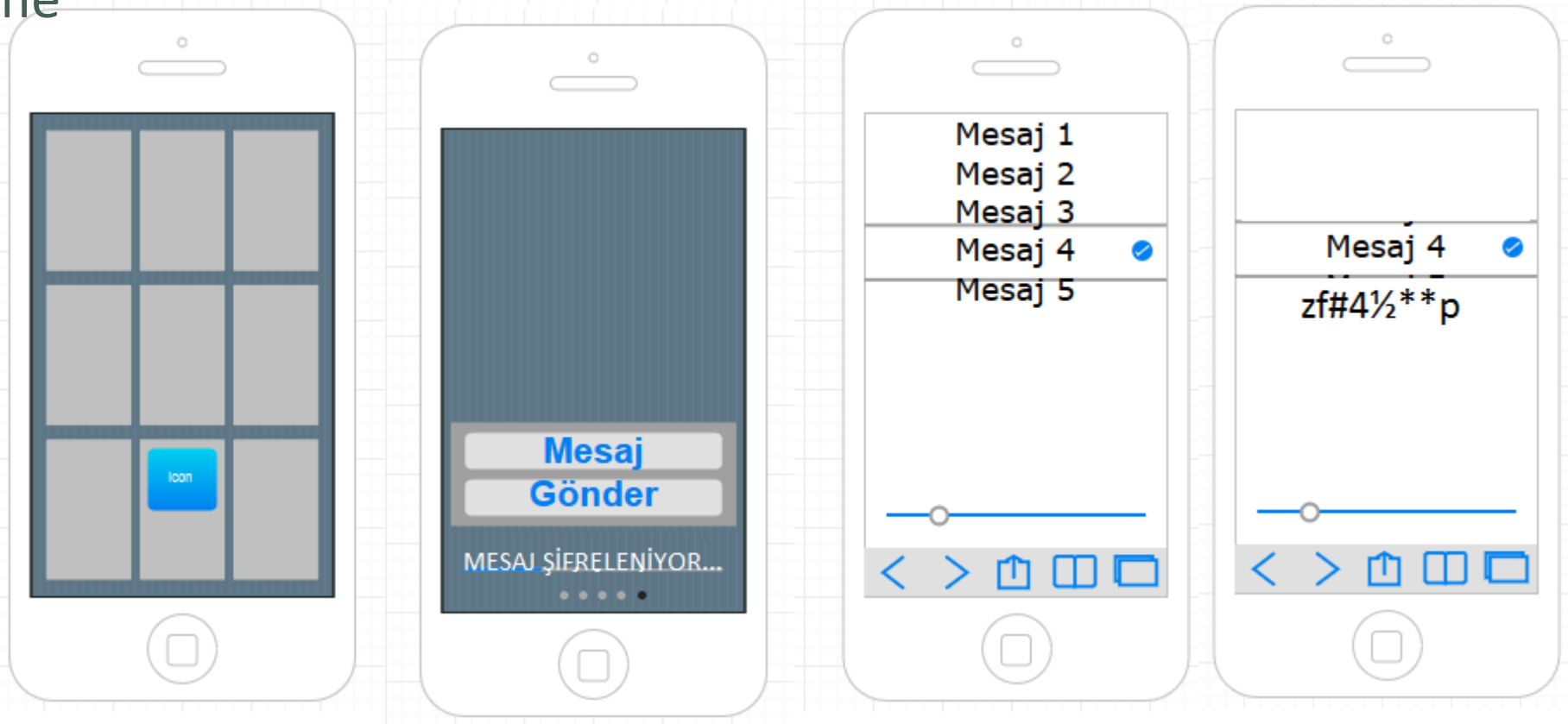


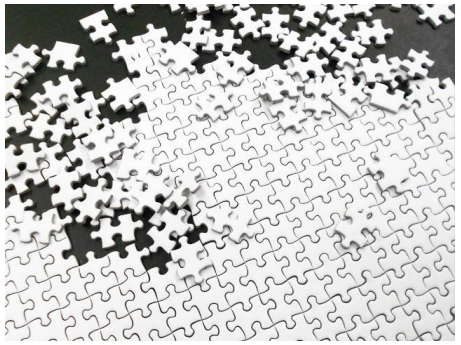


Proje

- Simetrik şifreleme
- Açık metin
- $Kullanıcı_A$
- $Kullanıcı_B$
- Şifreli metin

- Tasarımı
- Uygulama
- Test senaryosu





Araştırma + Sunum

- Bireysel
- Simetrik Şifreleme Algoritmaları
  - Standartlar
  - Analiz
  - Karşılaştırma