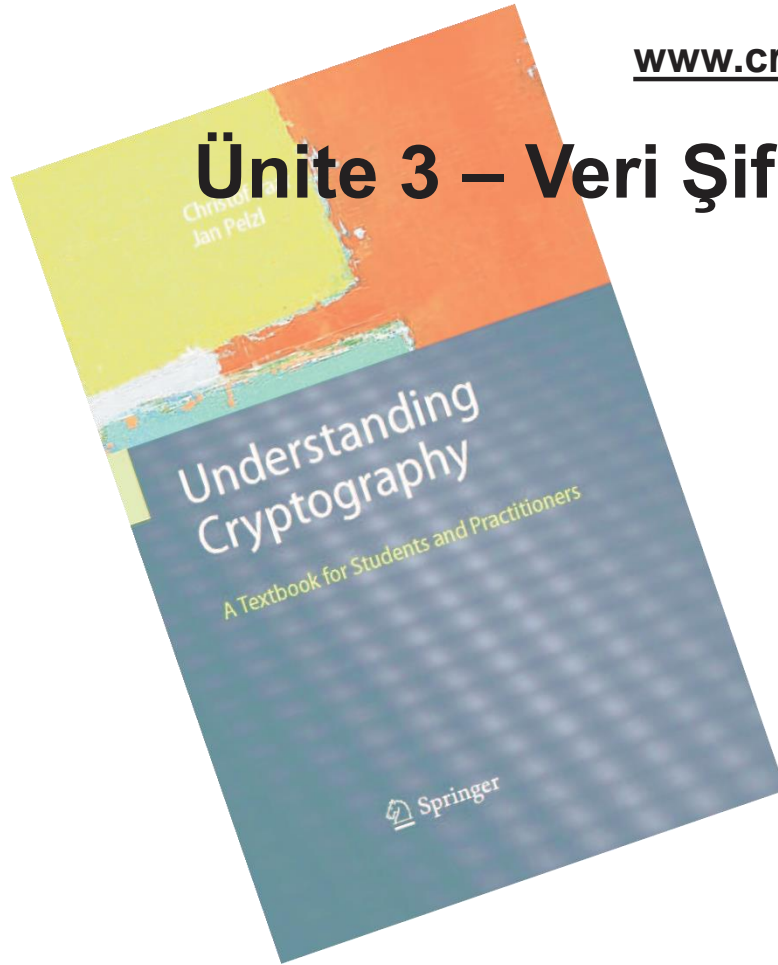


Understanding Cryptography Öğrenci ve Uygulamacılar İçin Ders kitabı

www.crypto-textbook.com

Ünite 3 – Veri Şifreleme Standardı (DES)



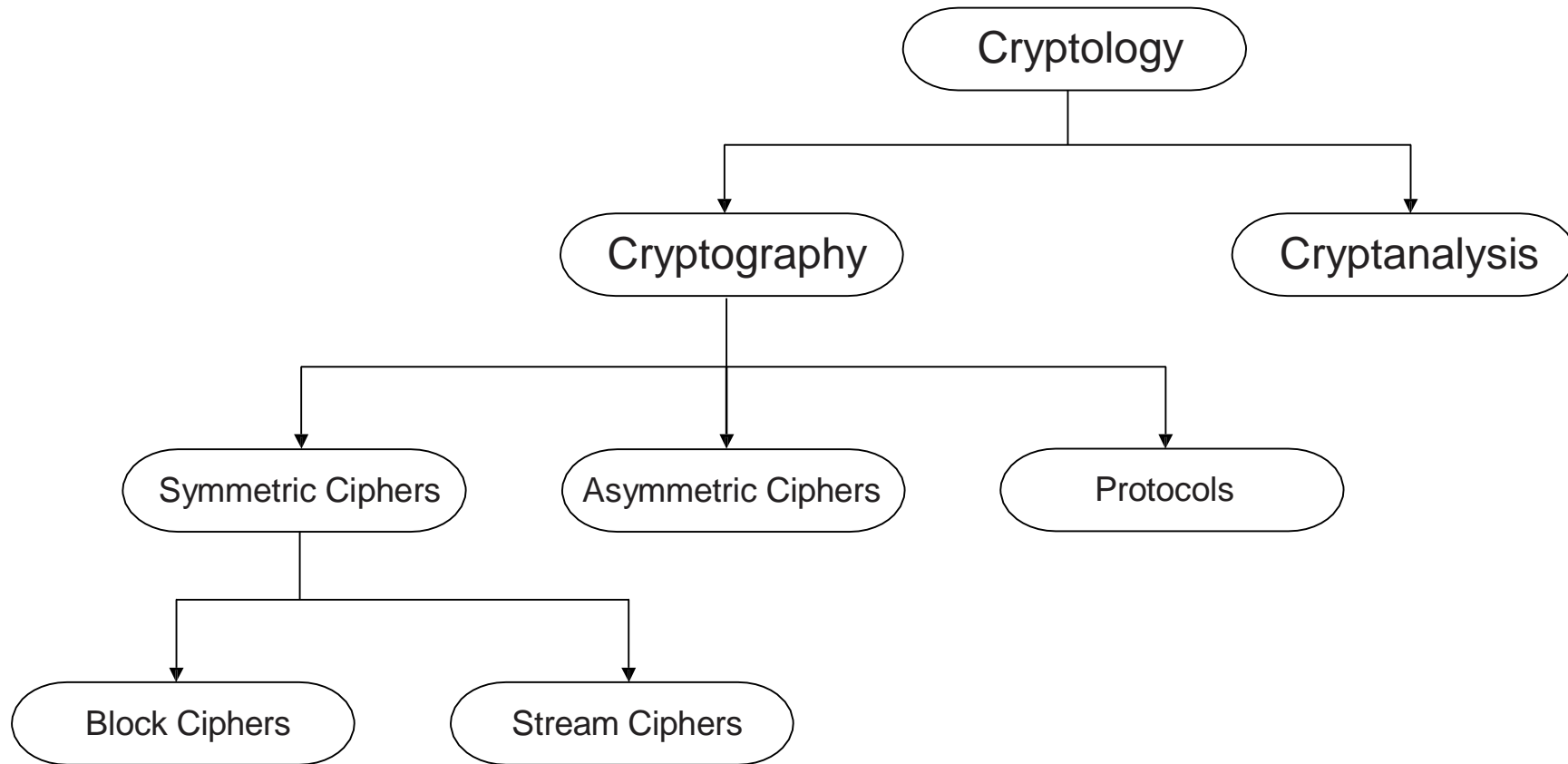
Ünite içeriği

- DES'e giriş
- DES Algoritmasına genel bakış
- DES'in iç yapısı
- Şifre çözme
- DES'in Güvenliği

Ünite içeriği

- **DES'e giriş**
- DES Algoritmasına genel bakış
- DES'in iç yapısı
- Şifre çözme
- DES'in Güvenliği

- Şifrelemede DES'in sınıflandırılması



DES burada yer alır

- **DES Gerçekleri**

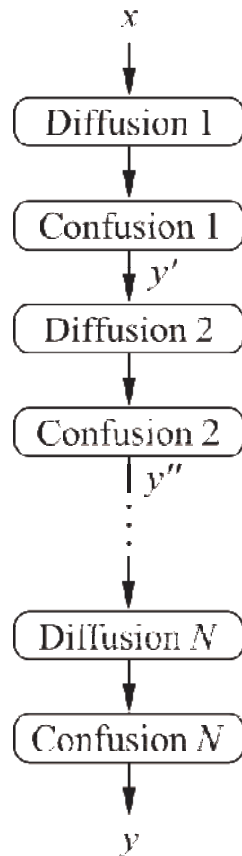
- DES **64 bit** uzunluktaki veri bloklarını şifreler.
- *Lucifer* şifreleme yapısını temel alarak **IBM** tarafından *National Security Agency* (NSA) (ulusal güvenlik acentesi)'nin etkisiyle geliştirildi, ve DES algoritmasının tasarlama kriterleri yayınlanmadı.
- Günümüzde *National Institute of Standards and Technology* (NIST) olarak ifade edilen **National Bureau of Standards** (NBS) tarafından **1977 de standartlaştırıldı.**
- Son 30 yılın en popüler **block şifreleme** yapısıdır.
- Bugüne kadar en çok çalışılan simetrik algoritmadır.
- Günümüzde **56 bitlik anahtar uzunluğu** güvenli değildir.
- **Fakat: 3DES güvenli bir şifreleme yapısı oluşturmuştur**, ve kullanımı hala yaygın.
- 2000 yılında *Advanced Encryption Standard* (**AES**) yer değiştirmiştir.
- Daha detaylı bilgi için Chapter 3.1 in *Understanding Cryptography* bakabilirsiniz.

- **Block Şifreleme Temelleri: Confusion and Diffusion**
- Claude Shannon: Güçlü şifreleme algoritmaları inşa edilebilmek için iki temel işlem vardır :
 1. **Confusion (karıştırma):** bir şifreleme işleminde **şifreli metin ile anahtar arasında bir ilişki olmamalıdır** .

Günümüzde, confusion işlemini sağlayan en yaygın yapı, AES ve DES'te yer alan **substitution (yer değiştirme)** işlemidir.
 2. **Diffusion (yayma):** Sabit yaklaşımları engellemek amacıyla düz metindeki bir sembolün şifreli metindeki bir çok sembolü etkilemesi işlemidir.

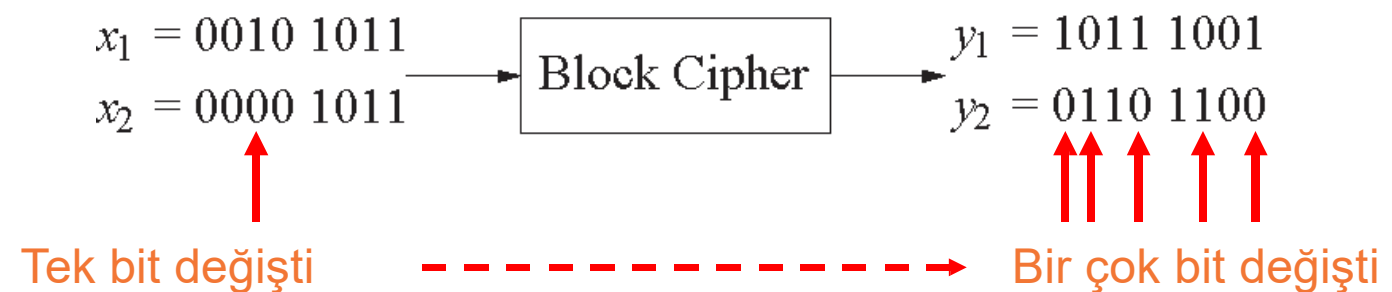
Basit bir difüzyon elemanı DES içinde sıklıkla kullanılan, **bit permutasyonudur**.
- İki işlemde kendi başlarına güvenliği sağlayamazlar. Buradaki amaç bu iki işlemi art arda kullanarak güvenli şifreler oluşturmaktır.

- **Ürün Şifreler**



- Bu gün kullanılan blok şifrelerin çoğu bu yapıları tekrar tekrar giriş verisine uygulayan round denilen yapılardan oluşur.
- Mükemmel difüzyon ulaşabilirsiniz: **Eğer düz metindeki bir biti değiştirdiğinizde ortalama olarak çıkış bitlerinin yarısını değiştiriyorsa.**

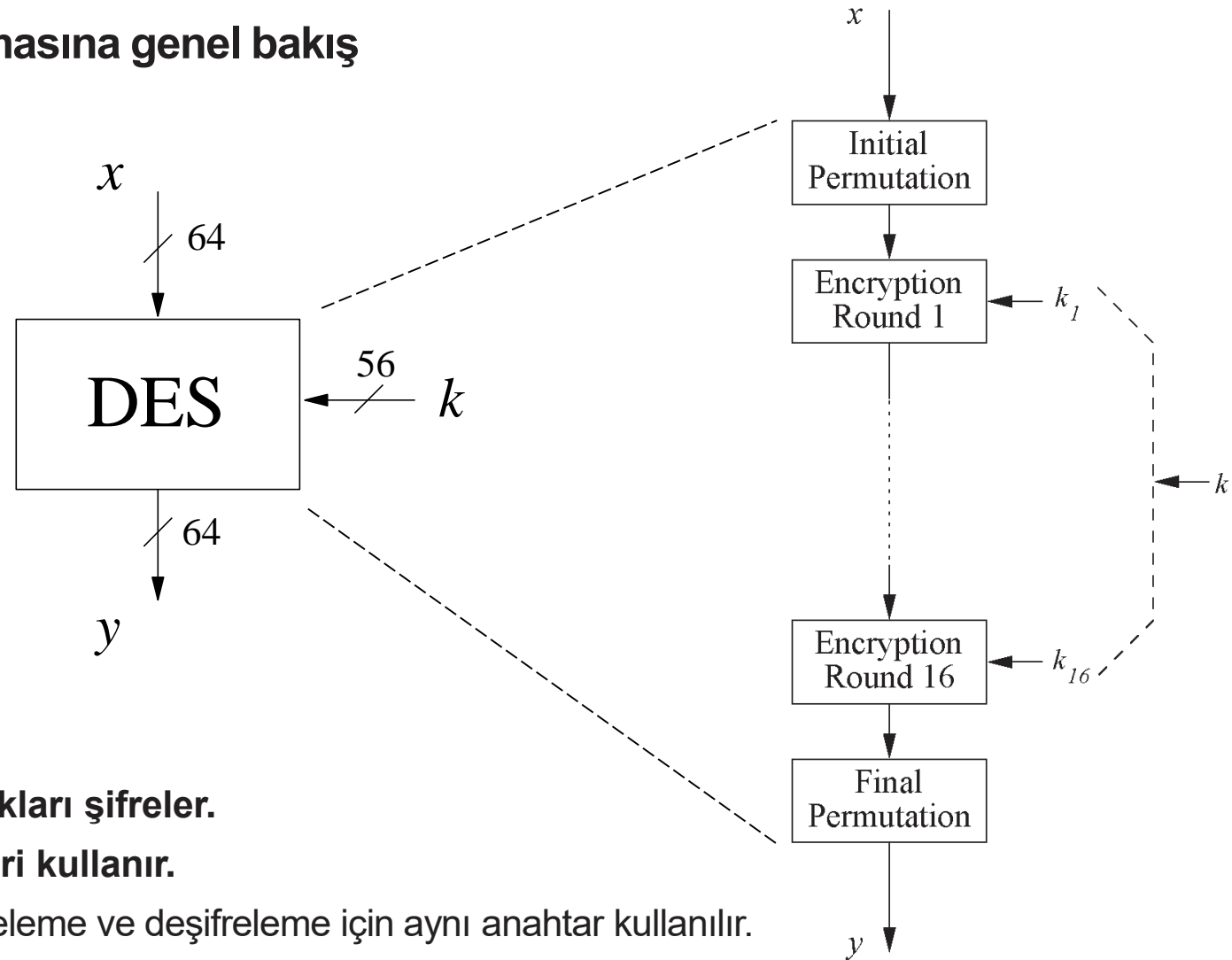
Örnek:



Ünite içeriği

- DES'e giriş
- **DES Algoritmasına genel bakış**
- DES'in iç yapısı
- Şifre çözme
- DES'in Güvenliği

- **DES Algoritmasına genel bakış**

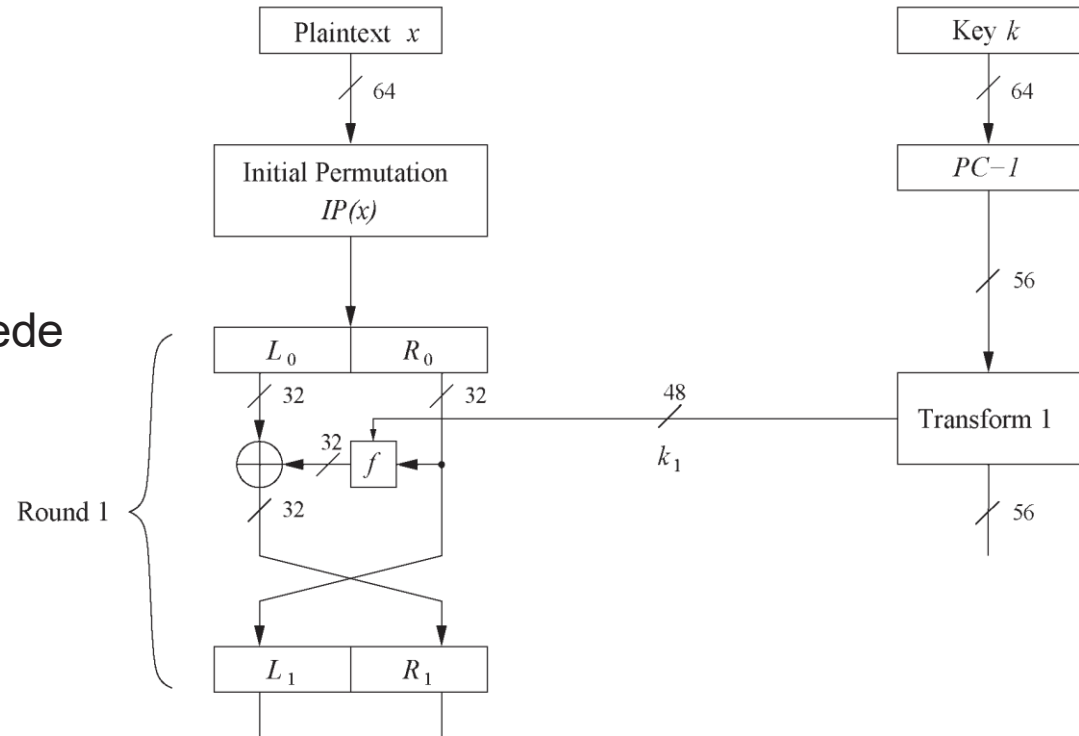


- **64 bit uzunluktaki blokları şifreler.**
- **56 bitlik anahtar değeri kullanır.**
- Simetrik şifreleme: şifreleme ve deşifreleme için aynı anahtar kullanılır.
- Aynı işlemleri yapan 16 round kullanılır
- Her roundda kullanılan farklı alt anahtarlar başlangıç anahtarından üretilir

- **DES Feistel Yapısı (1)**

- DES'in yapısı *Feistel yapısıdır*.

- Avantajı: şifreleme ve deşifrelemede sadece anahtar tarifesi farklıdır.



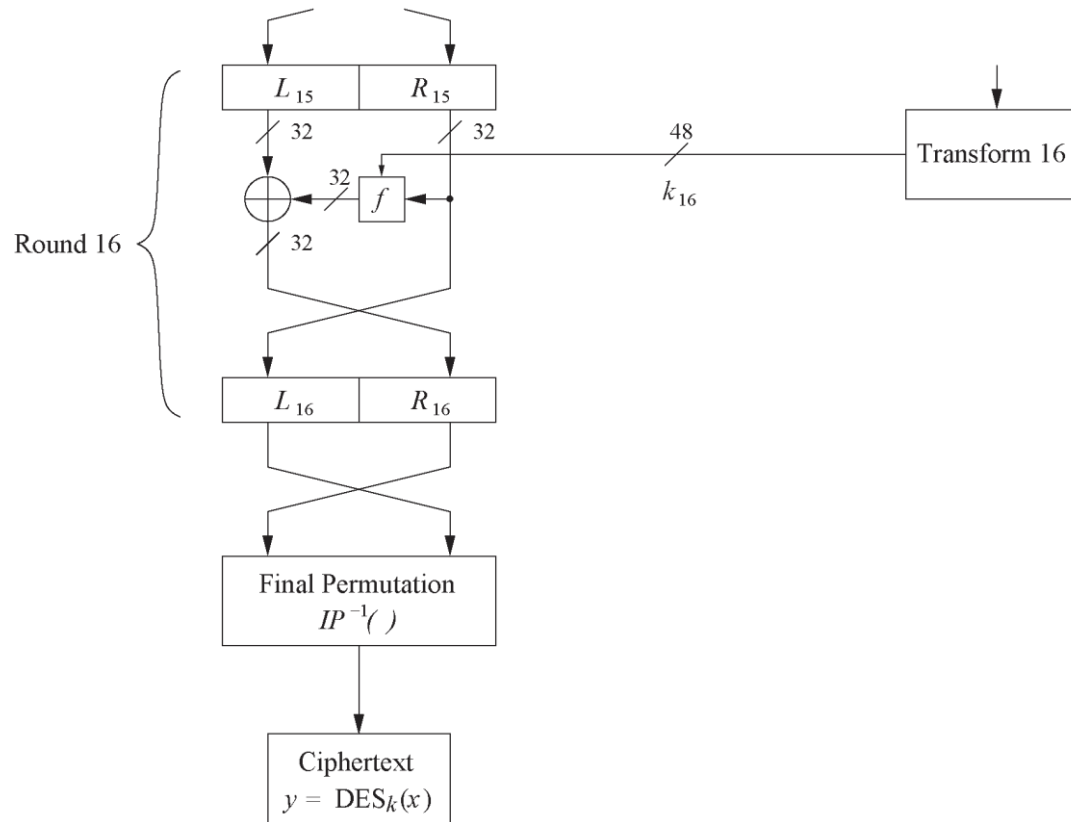
- Bit düzeyinde ilk permutasyon, ardından 16 round
 1. Düz metin 32-bitlik L_i ve R_i alt parçalarına ayrılır.
 2. R_i f fonksiyonuna varılır, bunun çıkışı L_i ile XOR'lanır.
 3. Sağ ve sol yarımlar yer değiştirir.
- Roundlar şöyle ifade edilebilir:

$$L_i = R_{i-1},$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

- **DES Feistel Yapısı (2)**

- L ve R 16. roundun sonunda tekrar yer değiştirir.



Ünite içeriği

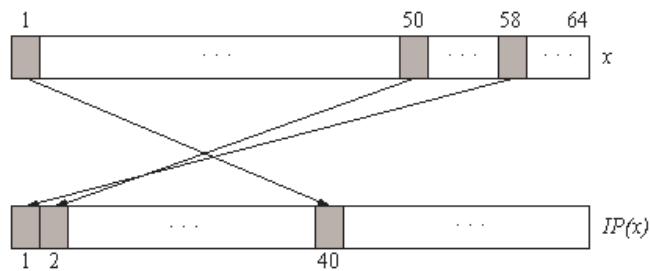
- DES'e giriş
- DES Algoritmasına genel bakış
- **DES'in iç yapısı**
- Şifre çözme
- DES'in Güvenliği

- **Başlangıç ve Son Permutasyon**

- Bit düzeyinde Permutasyon.
- Ters işlemler.
- IP ve IP^{-1} tablolarında gösterilmiştir.

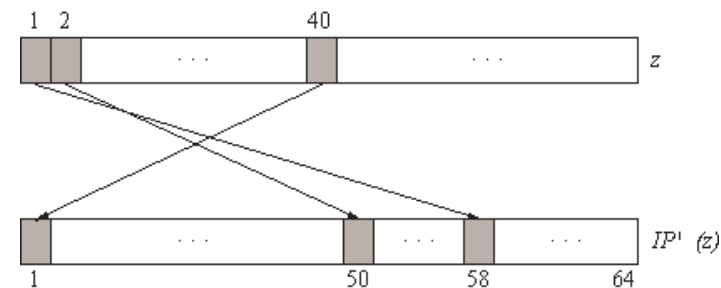
Başlangıç permutasyon

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			



Son permutasyon

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			



- **f-Fonksiyonu**

- **DES'in ana işlemleri**

- f -Fonksiyonu girişler:
 R_{i-1} ve round anahtarı k_i

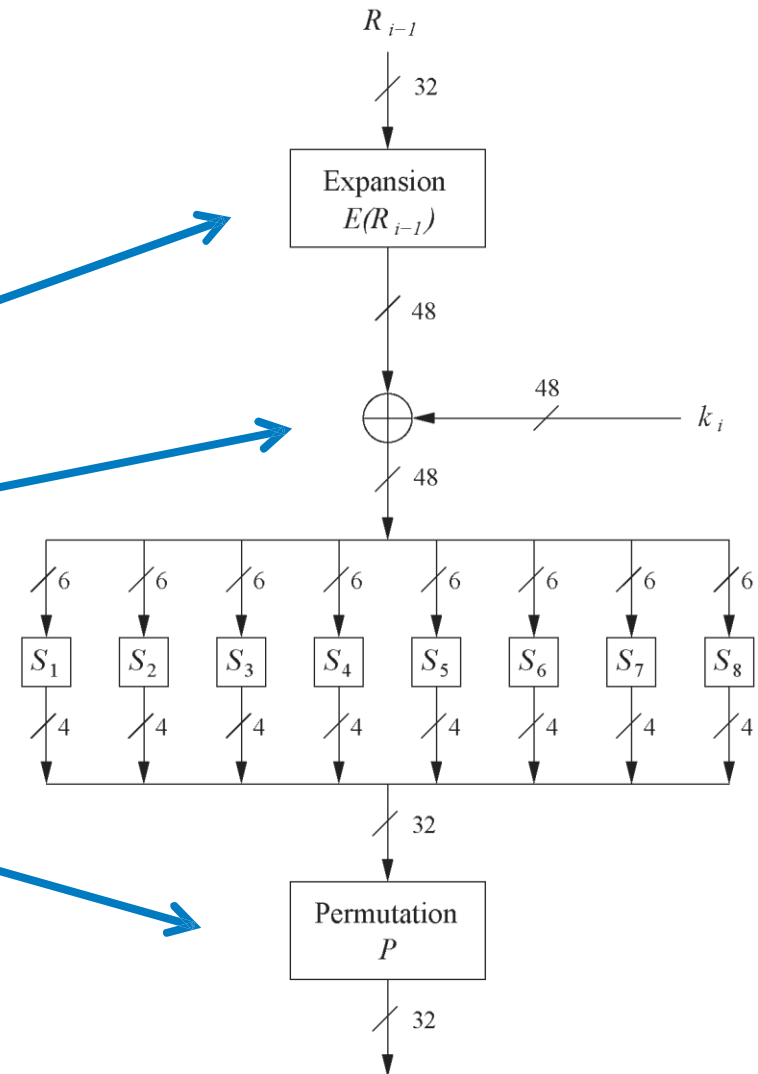
- **4 Adımlar:**

1. genişletilmiş E

2. Round anahtarı ile XOR

3. S-box substitution

4. Permütasyon

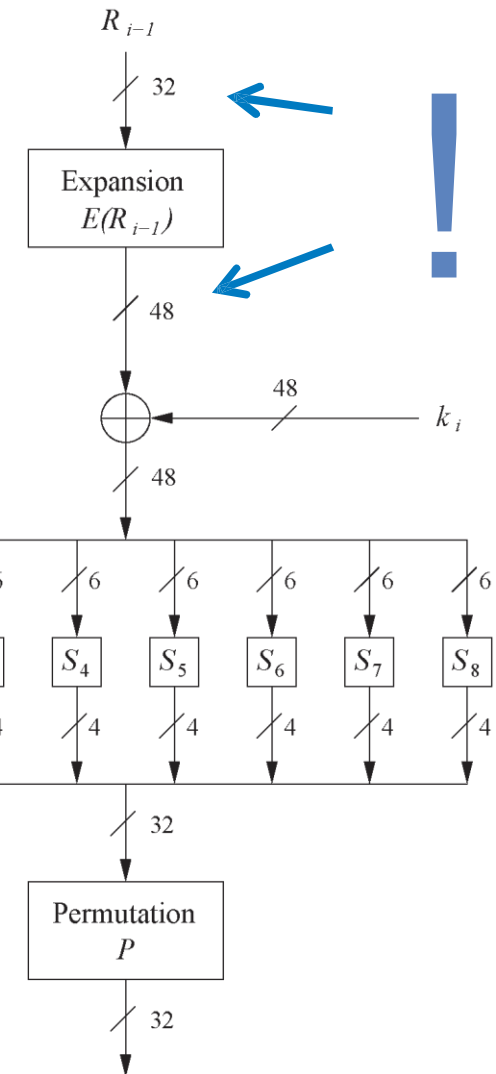
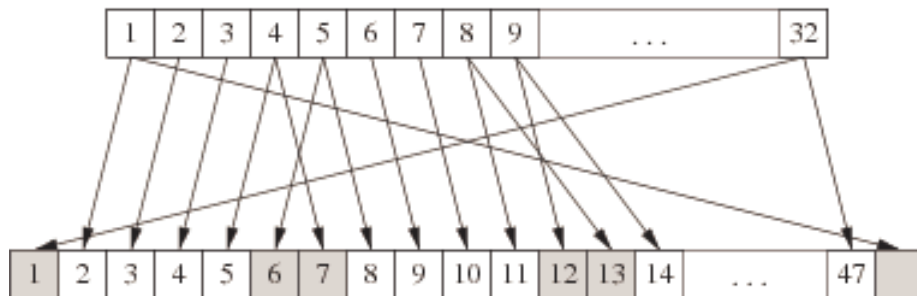


- Genişletme Fonksiyonu E

- Genişletilmiş E

- Temel amacı:
difizyonu artırmak

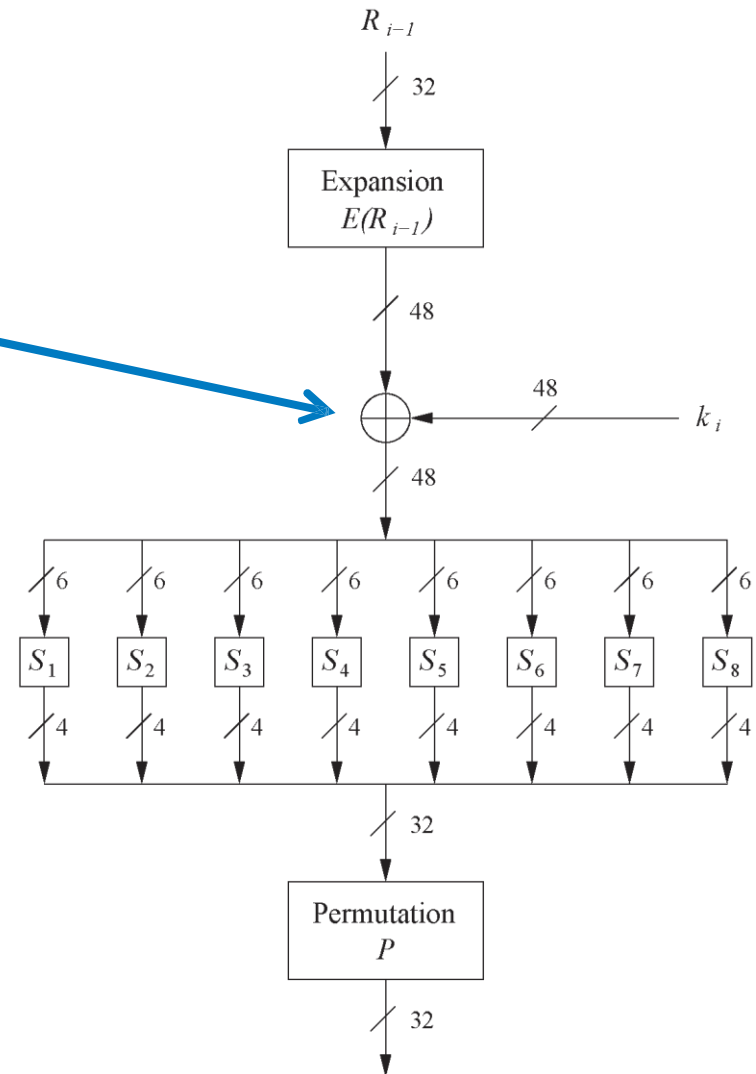
E												
32	1	2	3	4	5							
4	5	6	7	8	9							
8	9	10	11	12	13							
12	13	14	15	16	17							
16	17	18	19	20	21							
20	21	22	23	24	25							
24	25	26	27	28	29							
28	29	30	31	32	1							



- Round anahtarını ekleme

2. Round anahtarı XOR'lama

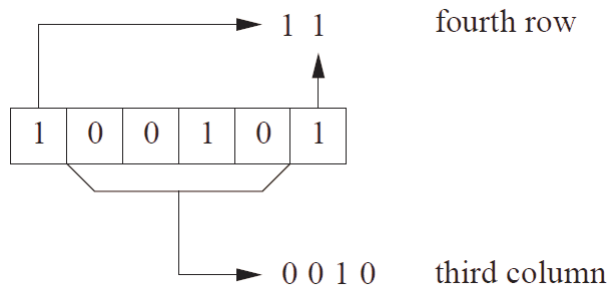
- *Round anahtarı ile genişletilmiş E 'nin çıkışı bit düzeyinde XOR'lanır.*
- **Rund anahtarı DES anahtar tarifesi ile başlangıç anahtarından üretilir. (ilerideki slaytlarda)**



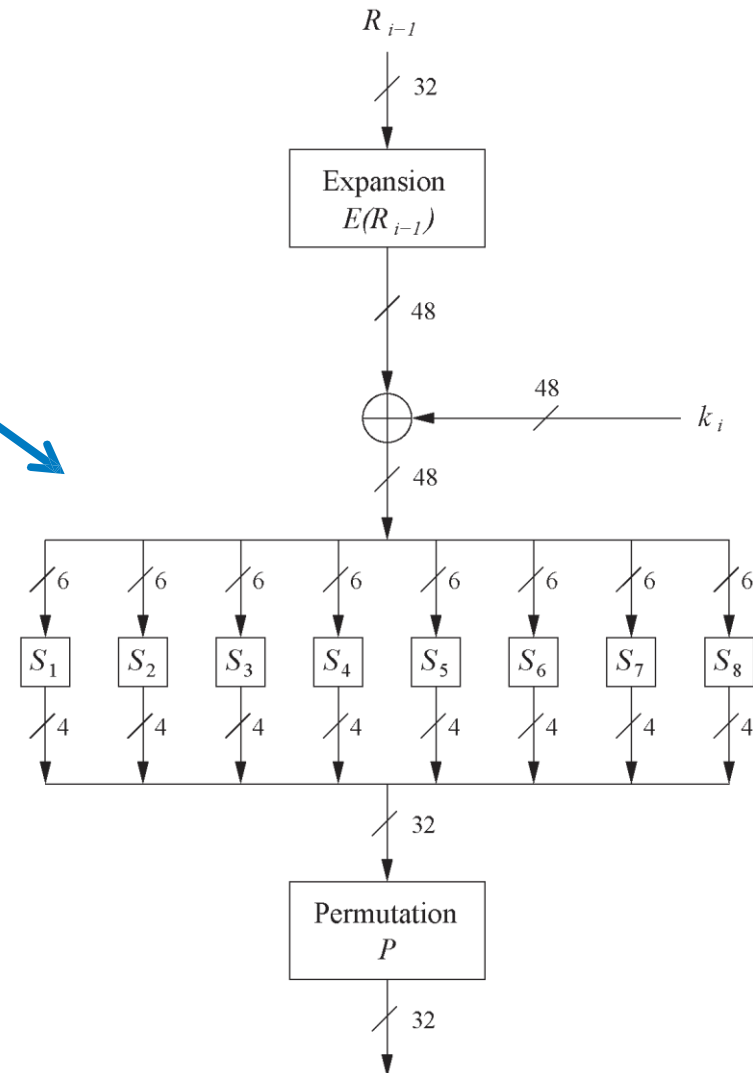
- **DES S-Box'ları**

3. S-Box substitution

- 8 substitution tablosu.
- 6 bits of input, 4 bits of output.
- Lineer değildir ve diferansiyel kriptanalize karşı dayanıklıdır.
- DES'in güvenliği için önemi yapar
- Bütün S-Box tabloları ve S-Box tasarlama kriterleri kaynak kitapta verilmiştir .



S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

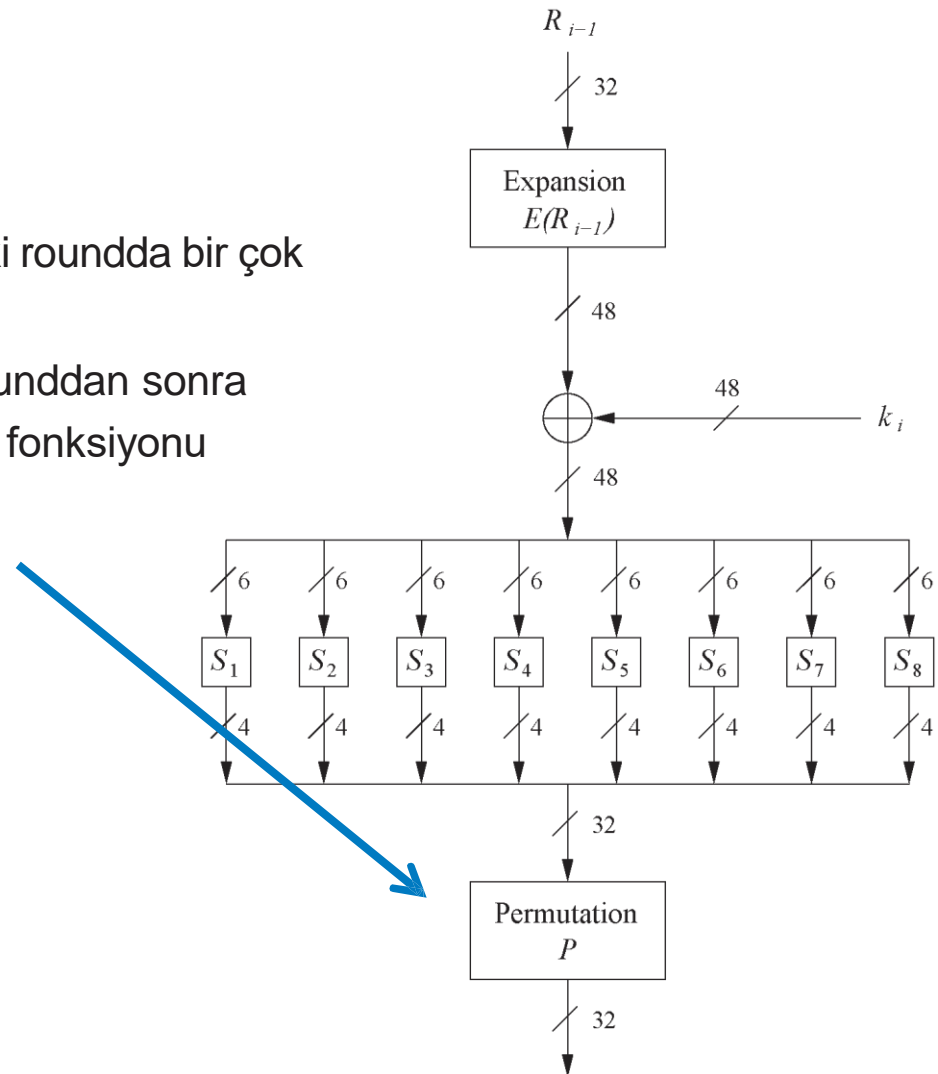


- **P permütasyonu**


4. Permutation P

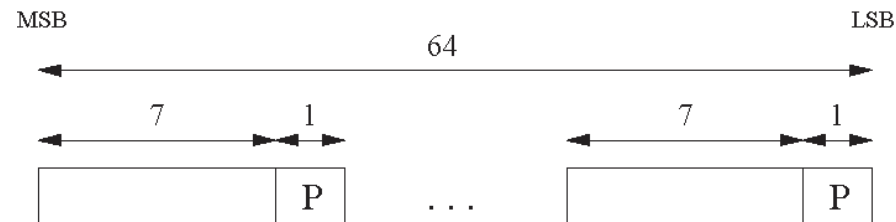
- Bit düzeyinde permütasyon.
- Difizyon tanıtımı.
- S-Box bitlerinin çıkışı bir sonraki roundda bir çok S-Boxları etkiler
- E difizyonu, S-Boxlar ve P 5 rounddan sonra her bit düz metnin ve anahtarın fonksiyonu olduğunu garanti eder.

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



- **Key Schedule (1)**

- 48 bitlik her k_i alt anahtarı orijinal 56 bitlik anahtardan oluşur.
- DES'te anahtar boyutu 64 bittir: burada **56 bit anahtar** ve 8 parity biti: 



P = parity bit

- **İlk permütasyon seçiminde parity bitleri kaldırılır PC-1:**
(bu kullanılmayan bitler 8, 16, 24, 32, 40, 48, 56 ve 64)

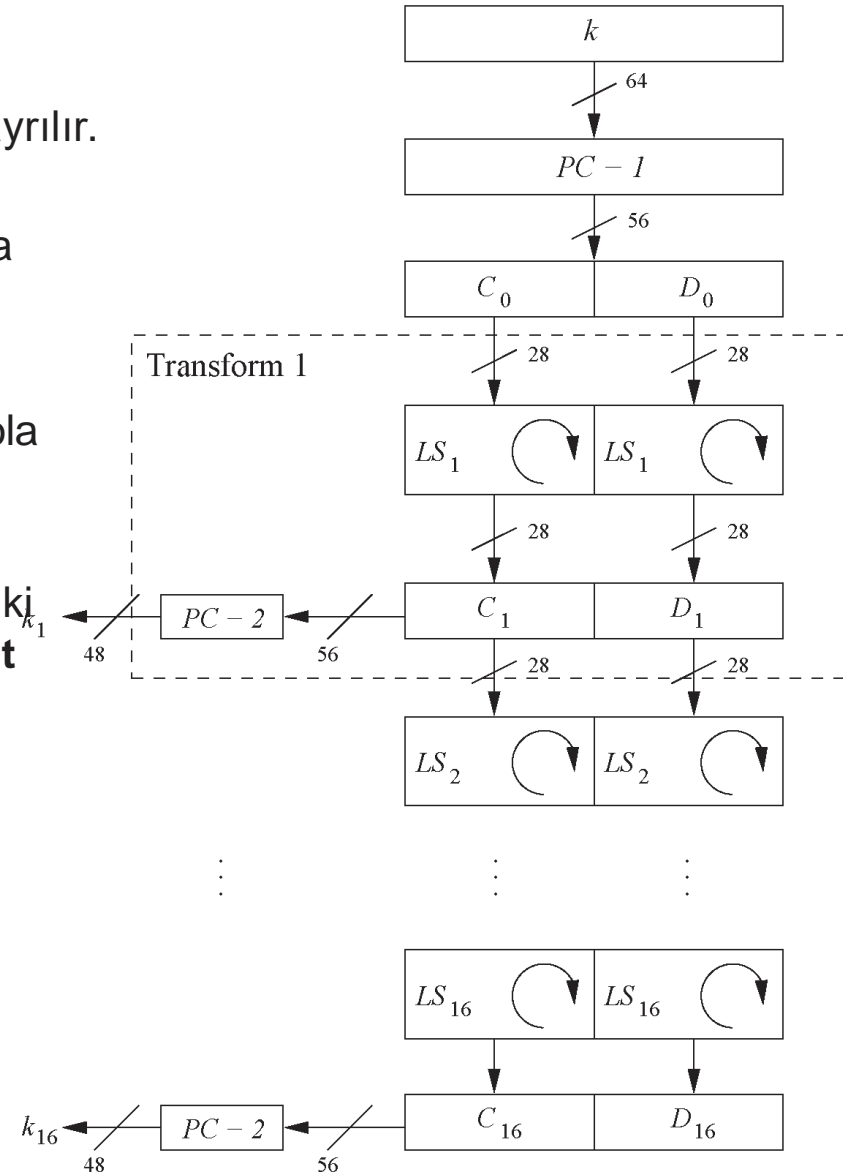
<i>PC - 1</i>							
57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	63	55	47	39
31	23	15	7	62	54	46	38
30	22	14	6	61	53	45	37
29	21	13	5	28	20	12	4

- **Key Schedule (2)**

- Anahtar C_0 ve D_0 denilen 28-bitlik iki parçaya ayrılır.
- $i = 1, 2, 9, 16$, numaralı roundlarda **bir bit** sola kaydırılır.
- **Diğer bütün roundlarda** her iki parça **iki bit** sola kaydırılır.
- her rounddaki anahtar değeri o rounddaki her iki anahtar yarısını kullanarak elde edilir. **Her k_i alt anahtarı K 'nın bir permütasyonudur!**

$PC - 2$							
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

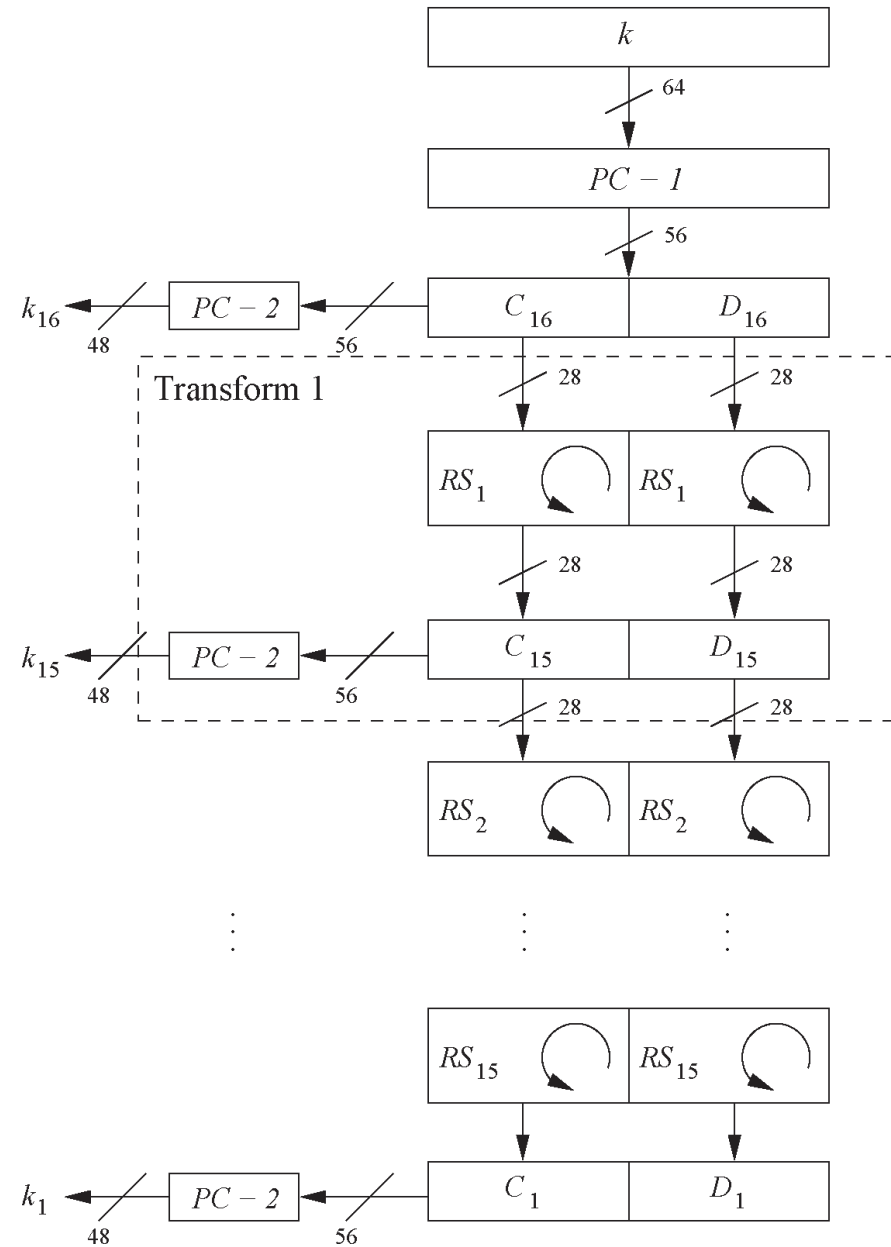
- **Not:** döndürmelerin toplam sayısı:
 $4 \times 1 + 12 \times 2 = 28 \Rightarrow D_0 = D_{16}$ and $C_0 = C_{16}$!



Ünite içeriği

- DES'e giriş
- DES Algoritmasına genel bakış
- DES'in iç yapısı
- **Şifre çözme**
- DES'in Güvenliği

- **deşifreleme**
- **Feistel şifrelemede** deşifreleme için sadece anahtar tarifiesi değiştirilir.
- Aynı 16 anahtar sırası ters çevrilerek üretilir.
- **Ters anahtar üretme:**
 $D_0=D_{16}$ ve $C_0=C_{16}$ yapılarak ilk anahtar üretilebilir.
 Her roundda anahtar üretim işlemlerinin tersi yapılır:
 - 1. rounda döndürme yok.
 - 2, 9 ve 16. roundda **bir bit sağa** kaydır.
 - Diğer roundlard **iki bit sağa** kaydırılır.



Ünite içeriği

- DES'e giriş
- DES Algoritmasına genel bakış
- DES'in iç yapısı
- Şifre çözme
- **DES'in Güvenliği**

- **DES'in Güvenliği**
- **DES önerildikten sonra iki önemli eleştiri yapıldı:**
 1. Anahtar uzayı çok küçük (2^{56} anahtar)
 2. S-box tasarlama kriterleri gizli tutuldu: sadece NSA tarafından bilinen herhangi bir gizlenmiş sayısal saldırı (*backdoors*), var mı?
- **Sayısal Saldırı:** DES yayınlandığı koşullarda linner ve diferansiyel kriptanalize oldukça dayanıklıydı. Bu IBM ve NASA'nın 15 yıldır bu saldırılardan haberdar olmuştu demektir!
Şimdiye kadar DES gerçekçi senaryolarla DES'i kırabilen bilinen analitik bir saldırı yoktur.
- **Ayrıntılı anahtar arama:** Şifresiz-şifreli her (x, y) çifti için deneme.

2^{56} anahtar vardır $DES_k(x)=y$ şartı sağlayana kadar.

⇒ Nispeten kolay bugünün bilgisayar teknolojisiyle!

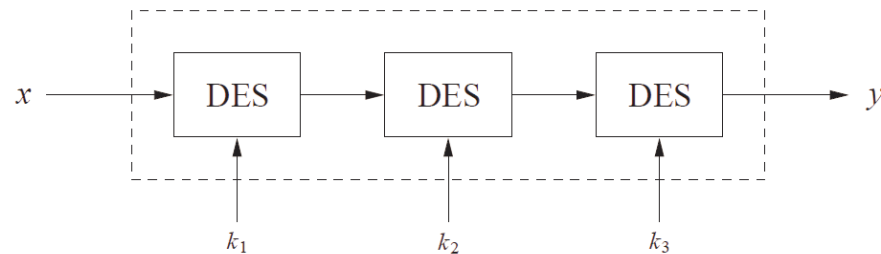
- **DES üzerindeki saldırıların tarihi**

Year	Proposed/ implemented DES Attack
1977	Diffie & Hellman, (under-)estimate the costs of a key search machine
1990	Biham & Shamir propose differential cryptanalysis (2^{47} chosen ciphertexts)
1993	Mike Wiener proposes design of a very efficient key search machine: Average search requires 36h. Costs: \$1.000.000
1993	Matsui proposes linear cryptanalysis (2^{43} chosen ciphertexts)
Jun. 1997	DES Challenge I broken, 4.5 months of distributed search
Feb. 1998	DES Challenge II--1 broken, 39 days (distributed search)
Jul. 1998	DES Challenge II--2 broken, key search machine <i>Deep Crack</i> built by the Electronic Frontier Foundation (EFF): 1800 ASICs with 24 search engines each, Costs: \$250 000, 15 days average search time (required 56h for the Challenge)
Jan. 1999	DES Challenge III broken in 22h 15min (distributed search assisted by <i>Deep Crack</i>)
2006-2008	Reconfigurable key search machine <i>COPACOBANA</i> developed at the Universities in Bochum and Kiel (Germany), uses 120 FPGAs to break DES in 6.4 days (avg.) at a cost of \$10 000.

- **Üçlü DES – 3DES**

- DES'in anahtar uzunluğunu etkili bir sayı olan 112 çıkarmak için DES algoritmasının üç defa kullanılmasına dayanır. Çoklu şifreleme ve anahtar uzunlukları hakkında daha fazla bilgi kaynak kitaptadır.

$$y = DES_{k_3}(DES_{k_2}(DES_{k_1}(x)))$$



- 3DES'in alternatif versiyonu: $y = DES_{k_3}(DES_{k_2}^{-1}(DES_{k_1}(x)))$.

Avantajı: $k_1=k_2=k_3$ seçilirse performans tek DES gibidir.

- Günümüzde daha pratik bir saldırı yok.
- Birçok eski uygulamalarda kullanılır., örneğin, banka sistemleri.

- **Alternatives to DES**

Algorithm	I/O Bit	key lengths	remarks
AES / Rijndael	128	128/192/256	DES "replacement", worldwide used standard
Triple DES	64	112 (effective)	conservative choice
Mars	128	128/192/256	AES finalist
RC6	128	128/192/256	AES finalist
Serpent	128	128/192/256	AES finalist
Twofish	128	128/192/256	AES finalist
IDEA	64	128	patented