Bilgi Güvenliği ve Kriptografi

DES (Data Encryption Standard)

- DES (Data Encryption Standard), 64 bitlik bloklar halinde şifreleme yapan bir blok şifreleyicisidir. 64 bitlik giriş bloğu için 64 bitlik çıkış bloğu elde edilir.

- DES simetrik bir algoritmadır. Şifreleme ve deşifreleme için aynı anahtar kullanılır. Anahtar uzunluğu 56 bit olup değiştirilmesi mümkündür (Anahtar 64 bittir, fakat her 8. bir parity (eşitlik) bitidir). Algoritmanın güvenliği anahtara bağlıdır.

- Algoritma iki tekniğin kombinasyonu şeklindedir. Bunlar *karıştırma* (confusion) ve *yayma* (diffusion) olarak ifade edilir. Bu tekniklerin basit bir birleşiminin bir blok üzerine uygulanması, *döngü* (round) olarak adlandırılır. DES 16 döngüye sahiptir.

- Daha açık bir ifadeyle, açık metnin bir bloğu üzerinde bu iki teknik 16 defa uygulanır

Eşitlik (Parity) Kodu

- İkili sayı sisteminde ifade edilen bilginin bir yerden başka bir yere taşınması dijital sistemlerde sıkça karşılaşılan bir olaydır. Bilginin bir yerden başka bölgeye taşınması sırasında, değişik nedenlerden dolayı gürültü oluşması ve oluşan gürültünün iletilen bilgiyi bozması zaman zaman karşılaşılan hadiselerdir.
- Hataları tespit etmede kullanılan en yaygın ve en kolay yöntem eşitlik biti kodlama (parity code) yöntemidir. Bu yöntemde, hataların ortaya çıkarılmasını sağlamak amacıyla BCD kodlu sayının sağındaki veya solundaki basamağa **'eşitlik biti'** (parity bit) eklenir. Eşitlik biti, kodlanan veride 1 yada 0'ların tek mi, çift mi olduğunu belirtir. İki türlü eşitlik biti yöntemi bulunmaktadır: Çift eşitlik (even parity) ve tek eşitlik (odd parity).
- **Çift eşitlik yönteminde;** eşitlik bitinin değeri, kodlanacak bilgideki 1'lerin toplam sayısı (eşitlik biti dahil) çift olacak şekilde seçilir. Kodlanacak sayıdaki 1'lerin sayısı tek ise, eşitlik biti olarak '1' eklenir. Kodlanacak bilgideki 1'lerin sayısı çift olması durumunda ise, eşitlik biti olarak '0' eklenir.

- Not: İkili veriler üzerinde işlem gören sistemler için aynı anda ancak bir bitin hatalı olabileceği iki bitin aynı anda hatalı olma olasılığının ihmal edilir düzeyde olduğu varsayımı yaygındır.

Çift eşitlik yöntemi

- $(1000011)_2$ sayısına çift eşitlik biti yöntemine göre eşitlik biti ekleyelim.
- Kodlanacak bilgide (1000011) üç adet '1' bulunduğundan, bilgideki 1'lerin sayısını çift yapmak için eşitlik biti olarak '1' eklenir ve sonuç olarak;
- (**1**1000011)
- sayısı oluşur.

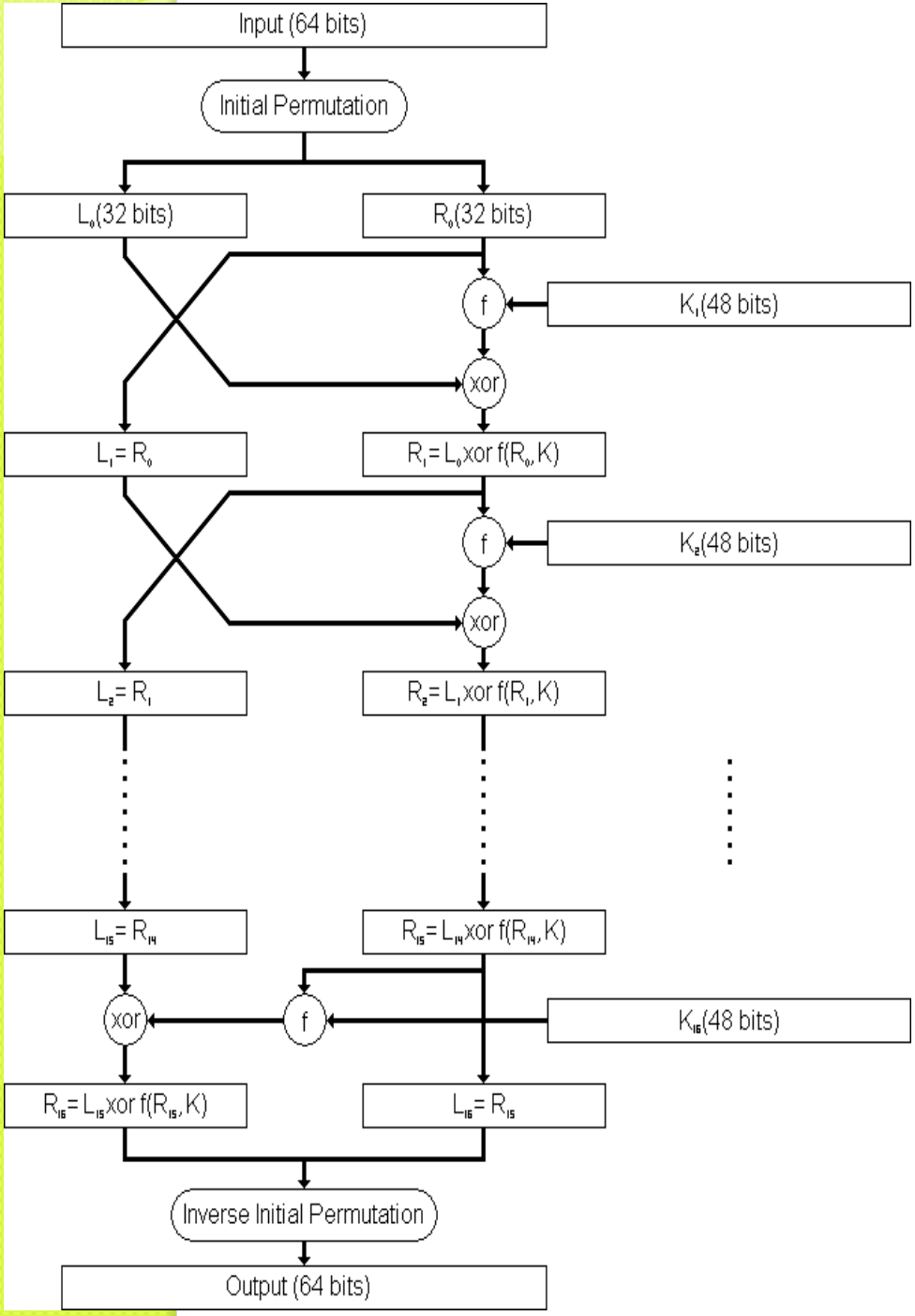
- $(1000001)_2$ sayısını çift eşitlik yöntemine göre kodlayalım.

- Verilen sayıda çift sayıda '1' bulunduğundan, eşitlik biti olarak '0' eklenir ve kodlama işlemi sonucunda;
  - '**0**1000001'
- bilgisi oluşur.

DES (Data Encryption Standard)

- DES giriş olarak aldığı 64 bitlik açık metin bloğuna, önce bir *başlangıç permütasyonu* (initial permutation) uygular ve ardından blok 32 bitlik iki alt bloğa bölünür.

- Bu alt bloklar üzerinde *f* fonksiyonu 16 defa uygulanır. Bu işlemde alt bloklar anahtar ile birleştirilir. İşlem sonunda alt bloklar birleştirilir ve başlangıçta uygulanan permütasyonun tersi uygulanarak algoritma sona erer.



Şekilde L_i sol yarı bloğu,

R_i sağ yarı bloğu,

K_i ise *i*. döngü için 48 bitlik anahtarı ifade etmektedir.

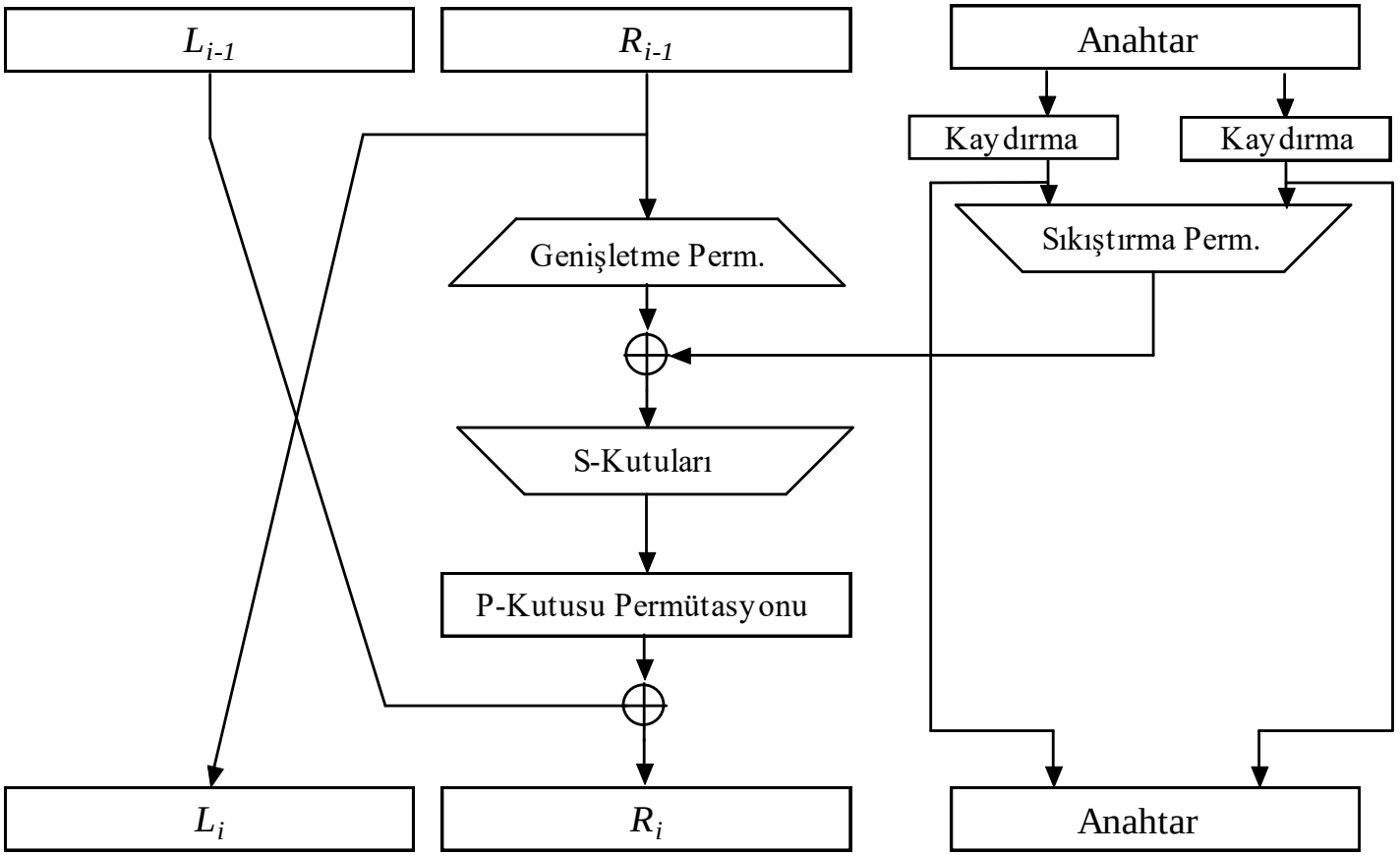
$L_i=R_{i-1}$,

$R_i=L_{i-1} \oplus f(R_{i-1},K_i)$'dir.

DES (Data Encryption Standard)

- Her döngüde anahtar bitleri kaydırılarak 56 bitten 48'i seçilir.
- Bloğun sağ yarısı *genişletme permütasyonu* (expansion permutation) ile 48 bite genişletilir ve XOR işlemi uygulanarak anahtarla birleştirilir.
- Elde edilen sonuç *S-kutularına* gönderilerek 32 yeni bit üretilir ve tekrar permütasyon işlemi uygulanır.
- Bu işlemler *f* fonksiyonunu oluşturur. *f*'nin çıkışı bloğun sol yarısı ile birleştirilerek (XOR) yeni sağ blok olarak atanır.
- Yeni sol blok ise sağ bloğun o döngü başlangıcındaki halidir(f uygulanmadan önceki)
- 16 tekrardan sonra bir sonraki 64 bitlik bloğa geçilir.

DES (Data Encryption Standard)



DES'in bir döngüsü

DES Aşamaları

- **Başlangıç Permütasyonu (Initial Permutation):** Bu permütasyon ve en son aşamada yapılan tersi permütasyon DES'in güvenliğine etki etmez. Bu permütasyonla bitlerin yerleri değiştirilir. Çoğu uygulamada bu işlem gerçekleştirilmez.

Başlangıç permütasyonu

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

DES Aşamaları

- **Anahtar Transformasyonu (Key Transformation):** Öncelikle 64 bitlik DES anahtarı 56 bite indirgenir. Bu işlem her 8. bitin yok edilmesiyle gerçekleştirilir. Bu bitler eşitlik kontrolü için kullanılabilir.

- 56 bitlik anahtar elde edildikten sonra DES'in her döngüsü için 48 bitlik farklı *alt anahtarlar* (subkey) üretilir. Bunlar K_i ile gösterilir ve aşağıdaki yöntemle oluşturulur.

  - 56 bitlik anahtar önce 28 bitlik iki parçaya ayrılır. Parçalar döngüsel olarak 1 ya da 2 bit kaydırılır. 16 döngü için kaydırılacak bit sayıları belirlenmiştir. Kaydırma işleminin ardından 56 bitten 48'i seçilir. Buna *sıkıştırma permütasyonu* (compression permutation) adı verilir. Kaydırmadan dolayı her alt anahtar farklı olmaktadır.

DES Aşamaları

Anahtar permütasyonu

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

Her döngüde kaydırılacak bit sayısı

Döngü	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Sayı	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Sıkıştırma permütasyonu

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

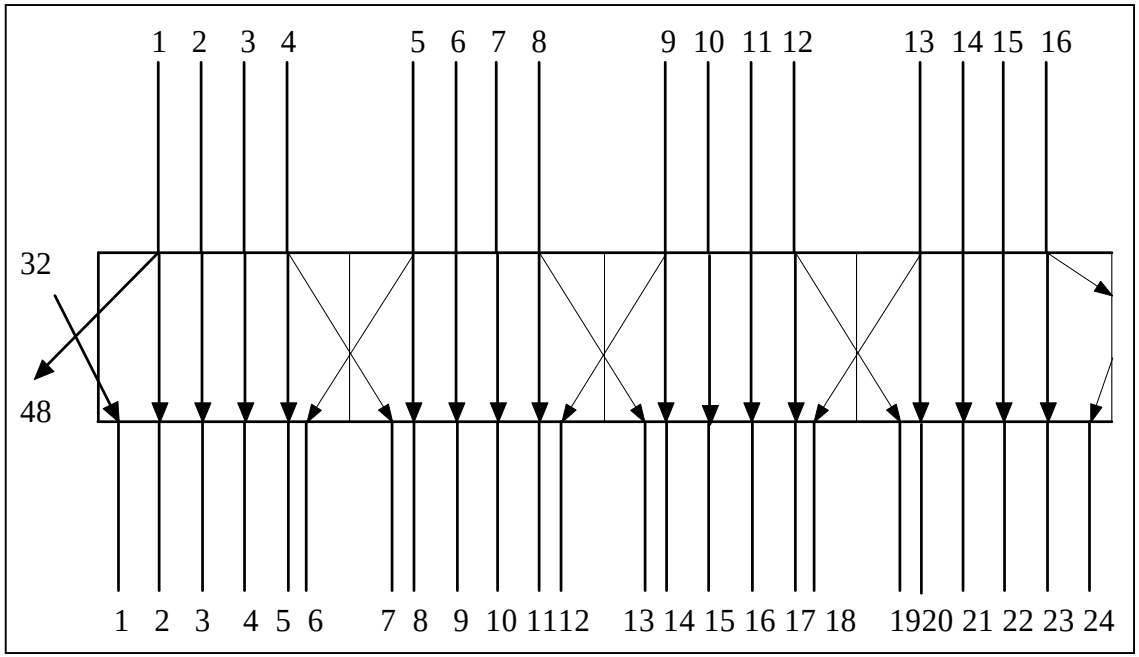
DES Aşamaları

- **Genişletme Permütasyonu (Expansion Permutation)**: Bu işlemle, bloğun sağ yarısı olan R_i, 32 bitten 48 bite genişletilerek, anahtarla aynı boyuta getirilir. Bu sayede, yer değiştirme işlemi süresince sıkıştırılabilecek daha uzun bir sonuç oluşturulur. Bu bazen *E-kutusu* (E-box) adını alır. Her 4 bitlik giriş bloğu için, 1. ve 4. bitlerin her biri, çıkış bloğunun iki bitini temsil eder. 2. ve 3. bitlerin her biri ise, çıkış bloğunun 1 bitini temsil eder. Tablo giriş pozisyonlarına karşılık gelen çıkış pozisyonlarını göstermektedir. Çıkış bloğu giriş bloğundan büyük olmasına rağmen, her giriş bloğu farklı bir çıkış bloğu üretmektedir.

DES Aşamaları

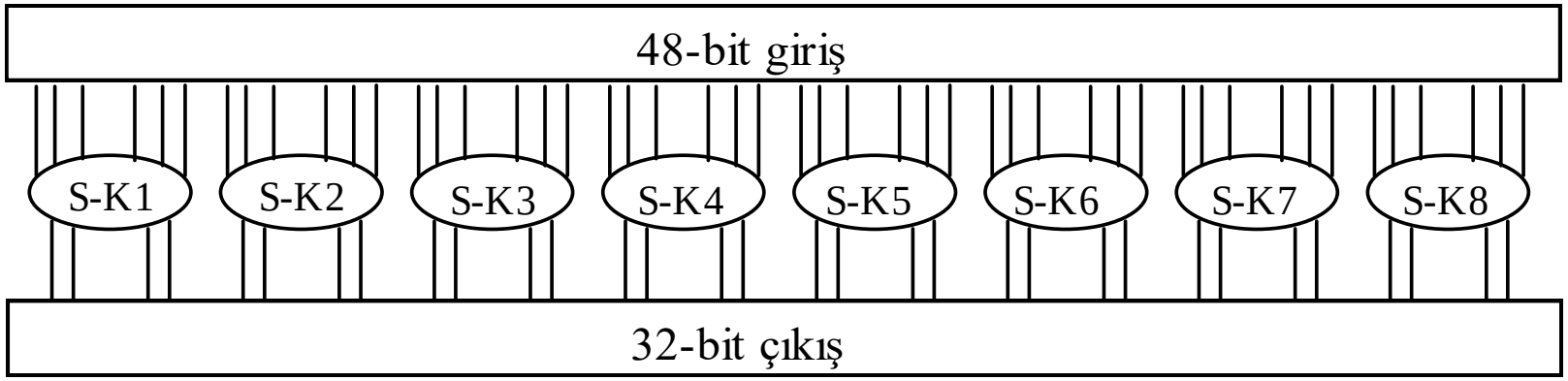
Genişletme permütasyonu

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



DES Aşamaları

- **S-kutuları ile Yerine Koyma (S-box Substitution):** Sıkıştırılmış anahtarın, genişletilen blokla XOR işlemine sokulmasıyla elde edilen 48 bitlik sonuç, yerine koyma işlemine tabi tutulur. Yerine koyma işlemi 8 adet *S-kutusu* ile yapılır. Her S-kutusu 6 bitlik girişe, 4 bitlik çıkışa sahiptir. Her blok ayrı bir S-kutusu ile işleme sokulur



DES Aşamaları

- S-kutuları 4 satırlı ve 16 sütunlu tablolardan oluşmaktadır. Kutudaki her çıkış 4 bitlik bir sayıdır. 6 bitlik giriş, çıkış için hangi satır ve sütuna bakılacağını belirler. $b_1b_2b_3b_4b_5b_6$ S-kutusu girişi olsun. b_1 ve b_6 birleştirilerek 0-3 arasında iki bitlik bir sayı oluşturulur. Bu sayı tablodaki satır numarasını belirler. Ortadaki 4 bit ise 4 bitlik bir sayı oluşturarak 0-15 arası sütun numarasını verir.

- Bu işlem, analizinin zor olması nedeniyle DES'in güvenliğini oluşturur. 8 adet 4 bitlik blokla oluşturulan 32 bitlik blok bir sonraki aşamanın girişine uygulanır.

DES Aşamaları

S-kutuları

S-Kutusu 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-Kutusu 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- Kutusu 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- Kutusu 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- Kutusu 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- Kutusu 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- Kutusu 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- Kutusu 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

DES Aşamaları

- **P-kutusu Permütasyonu (P-box Permutation):** S-kutusunun 32 bitlik çıkışı, *P-kutusuna* göre permütasyona tabi tutulur. Her giriş biti, bir çıkış pozisyonuna haritalanır ve hiçbir bit iki kere kullanılmaz yada göz ardı edilmez. Bitlerin hangi pozisyonlara haritalanacağı aşağıdaki tablo ile gösterilmektedir. Bu işlemin sonucu, 64 bitlik bloğun sol yarısı ile XOR'lanır. Sol ve sağ taraf yer değiştirilir ve bir sonraki döngü başlar.

P-kutusu permütasyonu

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

DES Aşamaları

- **Sonuç Permütasyonu (Final Permutation):** Bu, başlangıç permütasyonunun tersidir. Son döngüde sağ ve sol yarı yer değiştirmez, birleştirilir ve bu permütasyon işlemi uygulanır.

Sonuç permütasyonu

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

- Bütün bu işlemlerden sonra, deşifrelemenin şifrelemeden çok farklı olacağı düşünülebilir. Fakat aynı algoritma hem şifreleme hem de deşifreleme işlemini gerçekleştirmektedir. Deşifrelemede farklı olarak anahtarlar ters sırada kullanılmalıdır.