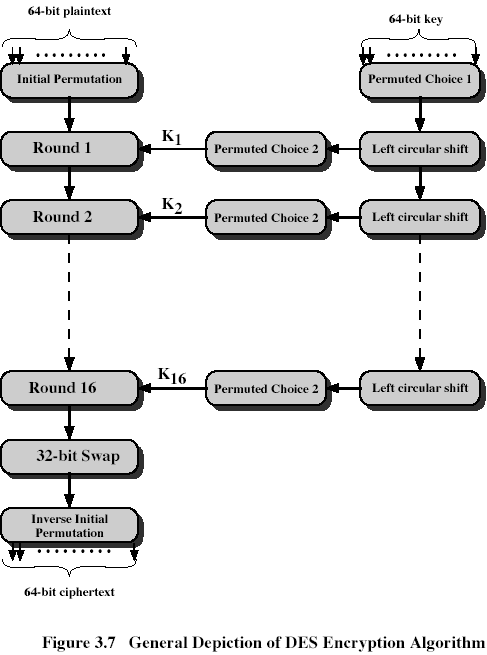
**VERİ ŞİFRELEME STANDARDI (DATA ENCRYPTION STANDARD, DES)**

1977'de Ulusal Standartlar Bürosu (NBS), şimdiki adıyla Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından Federal Bilgi İşleme Standardı 46 (FIPS PUB 46) olarak kabul edildi. 1971'de, Horst Feistel liderliğindeki IBM ekibi, 128 bitlik anahtarla 64 bitlik bloklarda çalışan LUCIFER algoritmasını geliştirdi. Ayrıca, Walter Tuchman ve Carl Meyer başkanlığındaki IBM ekibi, LUCIFER'ı kriptoanalize karşı daha dayanıklı hale getirmek için revize etti, ancak anahtar boyutunu 56 bite düşürdüler. 1973'te, NBS ulusal bir şifre standardı için teklif talebinde bulundu. IBM, Tuchman-Meyer projesinin sonuçlarını sundu. Bu, önerilen en iyi algoritmaydı ve 1977'de Veri Şifreleme Standardı olarak kabul edildi. 1994'te, NIST, DES'i 5 yıl daha federal kullanım için yeniden onayladı. 1999 yılında NIST, DES'in yalnızca eski sistemler için kullanılması gerektiğini ve üçlü DES'in kullanılması gerektiğini belirten standardının yeni bir versiyonunu (FIPS PUB 46-3) yayınladı.

**ŞİFRELEME DES**



32-bit takası sola kaydırır ve 16. Turdan sonra elde edilen 32-bit yarıları, ön çıktıyı elde ederiz. Son olarak, ön çıktı, 64-bit şifreli metni üretmek için başlangıç permütasyon IP'sinin tersi olan bir permütasyon IP -1'den geçer . Şekil 3.7'nin sağ tarafı, 56-bit'in nasıl kullanıldığını gösterir. 16 turun her biri için, bir sol dairesel kaydırma ve bir permütasyonun birleşimiyle bir alt anahtar Ki üretilir. Permütasyon fonksiyonu her tur için aynıdır.

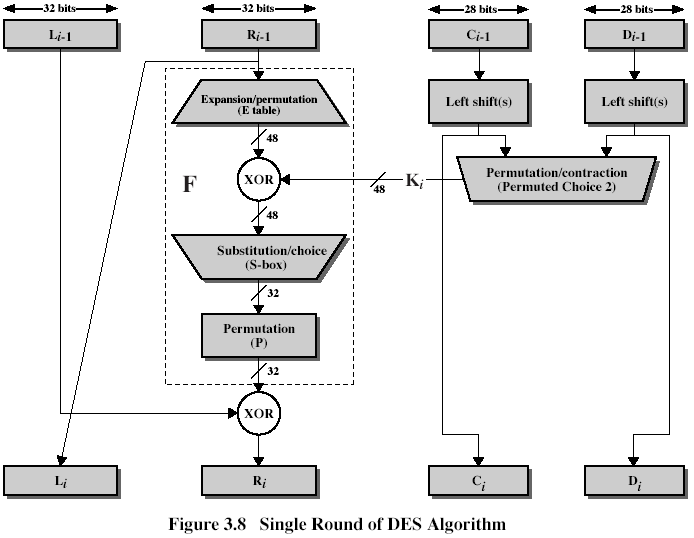
**BAŞLANGIÇ DEĞİŞİMİ VE TERS**

64 bitlik girişi etkiler

|  |
| --- |
| 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 |

**TEK TURUN DETAYLARI**



Her 64 bitlik ara değerin sol ve sağ yarıları, L ve R olarak etiketlenen ayrı 32 bitlik nicelikler olarak ele alınır. Klasik Feistel şifresinde olduğu gibi, her turdaki genel süreç aşağıdaki gibi özetlenir:



Yuvarlak anahtar Ki 48 bittir. R girişi 32 bittir. Bu R girişi ilk önce Genişleme/Permütasyon (E tablosu) ile 48 bite genişletilir:

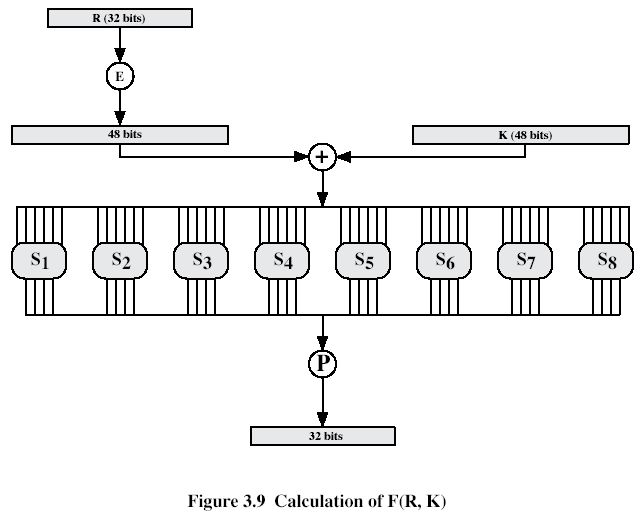
|  |  |  |
| --- | --- | --- |
| Genişleme/Permutasyon (E tablosu) | | |
| 32 | 1 2 3 4 | 5 |
| 4 | 5 6 7 8 | 9 |
| 8 | 9 10 11 12 | 13 |
| 12 | 13 14 15 16 | 17 |
| 16 | 17 18 19 20 | 21 |
| 20 | 21 22 23 24 | 25 |
| 24 | 25 26 27 28 | 29 |
| 28 | 29 30 31 32 | 1 |

**TEK TURUN DETAYLARI (DEVAMI 1)**

Elde edilen 48 bit, Ki ile XOR'lanır. Bu 48 bit sonuç, Permutasyon fonksiyonu (P) ile değiştirilen 32 bitlik çıktı üreten bir ikame fonksiyonundan geçer:

|  |
| --- |
| Permutasyon fonksiyonu (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 |

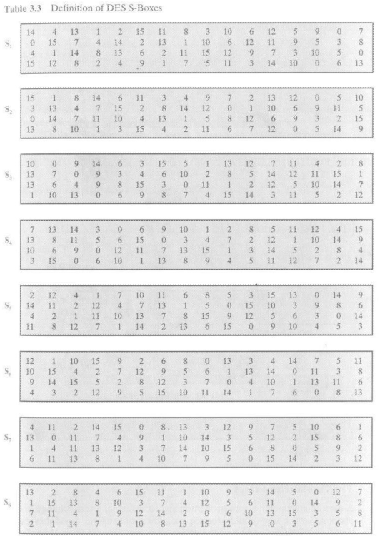
S-kutularının rolü Şekil 3.9'da gösterilmiştir:



İkame, her biri 6 bitlik girdi kabul eden ve çıkış olarak 4 bit üreten 8 S-kutusu kümesinden oluşur.

**TEK TURUN DETAYLARI (DEVAMI 2)**

Bu dönüşümler şunlardır:



S-kutusunun her satırı genel bir geri dönüşümlü ikameyi tanımlar: 6-bitlik giriş gruplarının her birinin ortadaki 4 biti S-kutusu çıkışıyla ikame edilir, 1. veson 6. bitlerdört bitten hangi özel ikamenin kullanılacağını tanımlar.

**ANAHTAR ÜRETİMİ**

Giriş anahtarı 64 bittir. Ancak her 8. bitkullanılmaz: 8,16,24,32,40,48,56,64 bitleri daha fazla kullanılmaz. 56 bitlik anahtar ilk önce permütasyona tabi tutulur Permutasyonlu Seçim 1:

|  |
| --- |
| Permutasyon Seçimi 1 (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 |

Elde edilen 56 bitlik anahtar daha sonra C0 ve D0 olarak etiketlenen iki 28 bitlik nicelik olarak ele alınır. Her turda, C i-1 ve D i-1, aşağıdakiler tarafından yönetilen 1 veya 2 bitlik dairesel bir sola kaydırmaya veya dönüşe ayrı ayrı tabi tutulur:

|  |
| --- |
| Sol Vardiya Takvimi |
| Yuvarlak sayı 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16  Bitler döndürüldü 1 1 2 2 2 2 2 2 2 1 2 2 2 2 2 2 1 |

Bu kaydırılmış değerler bir sonraki tura girdi olarak hizmet eder. Ayrıca, Permuted Choice 2'ye girdi olarak hizmet eder ve bu da fonksiyonuna girdi olarak hizmet eden 48 bitlik bir çıktı üretir .

|  |
| --- |
| Permutasyon Seçimi 2 (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 |

**ŞİFRE ÇÖZME**

Herhangi bir Feistel şifresinde olduğu gibi, şifre çözme işlemi şifreleme ile aynı algoritmayı kullanır; ancak alt anahtarların uygulanması terstir.

**DES'DE ÇIĞ ETKİSİ**

Düz metindeki 1 bitlik değişim şifreli metinde 34 bitlik farka yol açar. Anahtardaki 1 bitlik değişim şifreli metinde 35 bitlik farka yol açar.