DES'E ÖRNEK

Şimdi bir örnek üzerinde çalışıp, bazı sonuçlarını ele alalım. Örneği elle yapmanız beklenmese de, bir adımdan diğerine geçen onaltılık kalıpları incelemeyi bilgilendirici bulacaksınız.

Bu örnek için, düz metin onaltılık bir palindromdur. Düz metin, anahtar ve elde edilen şifreli metin aşağıdaki gibidir:

Plaintext:	`02468aceeca86420`
Key:	`0f1571c947d9e859`
Ciphertext:	`da02ce3a89ecac3b`

Sonuçlar

Tablo 4.2, algoritmanın ilerlemesini göstermektedir. İlk satır, ilk permütasyondan sonra verinin sol ve sağ yarısının 32 bitlik değerlerini gösterir. Sonraki 16 satır, her turdan sonra sonuçları gösterir. Ayrıca, her tur için oluşturulan 48 bit alt anahtarının değeri de gösterilir. $L_i = R_{i-1}$ olduğuna dikkat edin.Son satır ters ilk permütasyondan (inverse initial permutation) sonra sol ve sağdaki değerleri gösterir. Birleştirilen bu iki değer şifreli metni oluşturur.

Tablo 4.2 DES Örneği

Round	*Ki*	*Li*	*Ri*
IP		5a005a00	3cf03c0f
1	1e030f03080d2930	3cf03c0f	bad22845
2	0a31293432242318	bad22845	99e9b723
3	23072318201d0c1d	99e9b723	0bae3b9e
4	05261d3824311a20	0bae3b9e	42415649
5	3325340136002c25	42415649	18b3fa41
6	123a2d0d04262a1c	18b3fa41	9616fe23
7	021f120b1c130611	9616fe23	67117cf2
8	1c10372a2832002b	67117cf2	c11bfc09
9	04292a380c341f03	c11bfc09	887fbc6c
10	2703212607280403	887fbc6c	600f7e8b
11	2826390c31261504	600f7e8b	f596506e
12	12071c241a0a0f08	f596506e	738538b8
13	300935393c0d100b	738538b8	c6a62c4e
14	311e09231321182a	c6a62c4e	56b0bd75
15	283d3e0227072528	56b0bd75	75e8fd8f
16	2921080b13143025	75e8fd8f	25896490
IP–1		da02ce3a	89ecac3b

Not: DES alt anahtarları hex formatında sekiz 6 bitlik değer olarak gösterilir.

DES'DEKİ ÇIĞ ETKİSİ (AVALANCHE EFFECT)

Herhangi bir şifreleme algoritmasının istenen bir özelliği, düz metin veya anahtardaki küçük bir değişikliğin şifreli metinde önemli bir değişiklik üretmesi gerektiğidir. **Özellikle, düz metnin bir bitindeki veya anahtarın bir bitindeki bir değişiklik, şifreli metnin birçok bitinde değişiklik üretmelidir. Bu çığ etkisi (avalanche effect) olarak adlandırılır.**

Burada, düz metindeki (Plaintext) 1 bitlik değişiklik şifreli metinde (cipher-text) 34 bitlik farklılığa neden olur. Anahtardaki 1 bitlik değişiklik şifreli metinde 35 bitlik farklılığa neden olur.

Değişiklik küçükse, bu, aranacak düz metin veya anahtar alanın boyutunu azaltmanın bir yolunu sağlayabilir.

Tablo 4.2'deki örneği kullanarak, Tablo 4.3, düz metnin 12468aceeca86420 olması durumunda, düz metnin dördüncü biti değiştirildiğinde olan sonucu göstermektedir. Tablonun ikinci sütunu, iki düz metin için her bir turun sonundaki ara 64 bitlik değerleri göstermektedir. Üçüncü sütun, iki ara değer arasında farklılık gösteren bit sayısını gösterir. **Tablo, sadece üç turdan sonra, iki bit arasında 18 bitin farklı olduğunu göstermektedir. Tamamlandığında, iki şifre metni 32 bit pozisyonda farklıdır.**
Tablo 4.4, yalnızca dördüncü bit konumunda farklılık gösteren iki anahtarın orijinal düz metnini kullanan benzer bir testi gösterir: orijinal anahtar, 0f1571c947d9e859 ve değiştirilmiş anahtar, 1f1571c947d9e859. Yine sonuçlar, şifreli metindeki bitlerin yaklaşık yarısının farklı olduğunu ve çığ etkisinin sadece birkaç turdan sonra telaffuz edildiğini göstermektedir.

Tablo 4.3 DES'te Çığ Etkisi: Plaintext Değişimi

Round		δ
	02468aceeca86420 12468aceeca86420	1
1	3cf03c0fbad22845 3cf03c0fbad32845	1
2	bad2284599e9b723 bad3284539a9b7a3	5
3	99e9b7230bae3b9e 39a9b7a3171cb8b3	18
4	0bae3b9e42415649 171cb8b3ccaca55e	34
5	4241564918b3fa41 ccaca55ed16c3653	37
6	18b3fa419616fe23 d16c3653cf402c68	33
7	9616fe2367117cf2 cf402c682b2cefbc	32
8	67117cf2c11bfc09 2b2cefbc99f91153	33

Round		δ
9	c11bfc09887fbc6c 99f911532eed7d94	32
10	887fbc6c600f7e8b 2eed7d94d0f23094	34
11	600f7e8bf596506e d0f23094455da9c4	37
12	f596506e738538b8 455da9c47f6e3cf3	31
13	738538b8c6a62c4e 7f6e3cf34bc1a8d9	29
14	c6a62c4e56b0bd75 4bc1a8d91e07d409	33
15	56b0bd7575e8fd8f 1e07d4091ce2e6dc	31
16	75e8fd8f25896490 1ce2e6dc365e5f59	32
IP–1	da02ce3a89ecac3b 057cde97d7683f2a	32

Tablo 4.4 DES'te Çığ Etkisi: Anahtar Değişimi

Round		δ
	02468aceeca86420 02468aceeca86420	0
1	3cf03c0fbad22845 3cf03c0f9ad628c5	3
2	bad2284599e9b723 9ad628c59939136b	11
3	99e9b7230bae3b9e 9939136b768067b7	25
4	0bae3b9e42415649 768067b75a8807c5	29
5	4241564918b3fa41 5a8807c5488dbe94	26
6	18b3fa419616fe23 488dbe94aba7fe53	26
7	9616fe2367117cf2 aba7fe53177d21e4	27
8	67117cf2c11bfc09 177d21e4548f1de4	32

Round		δ
9	c11bfc09887fbc6c 548f1de471f64dfd	34
10	887fbc6c600f7e8b 71f64dfd4279876c	36
11	600f7e8bf596506e 4279876c399fdc0d	32
12	f596506e738538b8 399fdc0d6d208dbb	28
13	738538b8c6a62c4e 6d208dbbb9bdeeaa	33
14	c6a62c4e56b0bd75 b9bdeeaad2c3a56f	30
15	56b0bd7575e8fd8f d2c3a56f2765c1fb	33
16	75e8fd8f25896490 2765c1fb01263dc4	30
IP^{-1}	da02ce3a89ecac3b ee92b50606b62b0b	30