LİNEER KRİPTANALİZ

1. DENEYİN AMACI

Bu deney, simetrik şifreleme algoritması kullanılarak şifrelenmiş bir metnin, üçüncü bir kişi (düşman) tarafından lineer kriptanaliz yöntemi ile nasıl çözülebileceğini göstermeyi amaçlamaktadır. Şifre kırma yöntemi olarak gösterilecek olan lineer kriptanaliz, [1] dokümanında detaylı olarak açıklanmıştır. Burada amaç lineer kriptanalizi öğretmek olduğundan, üzerinde kriptanaliz yapılabilecek basitleştirilmiş bir şifreleme algoritması seçilmiştir.

2. DES (Data Encryption Standard) ALGORİTMASI

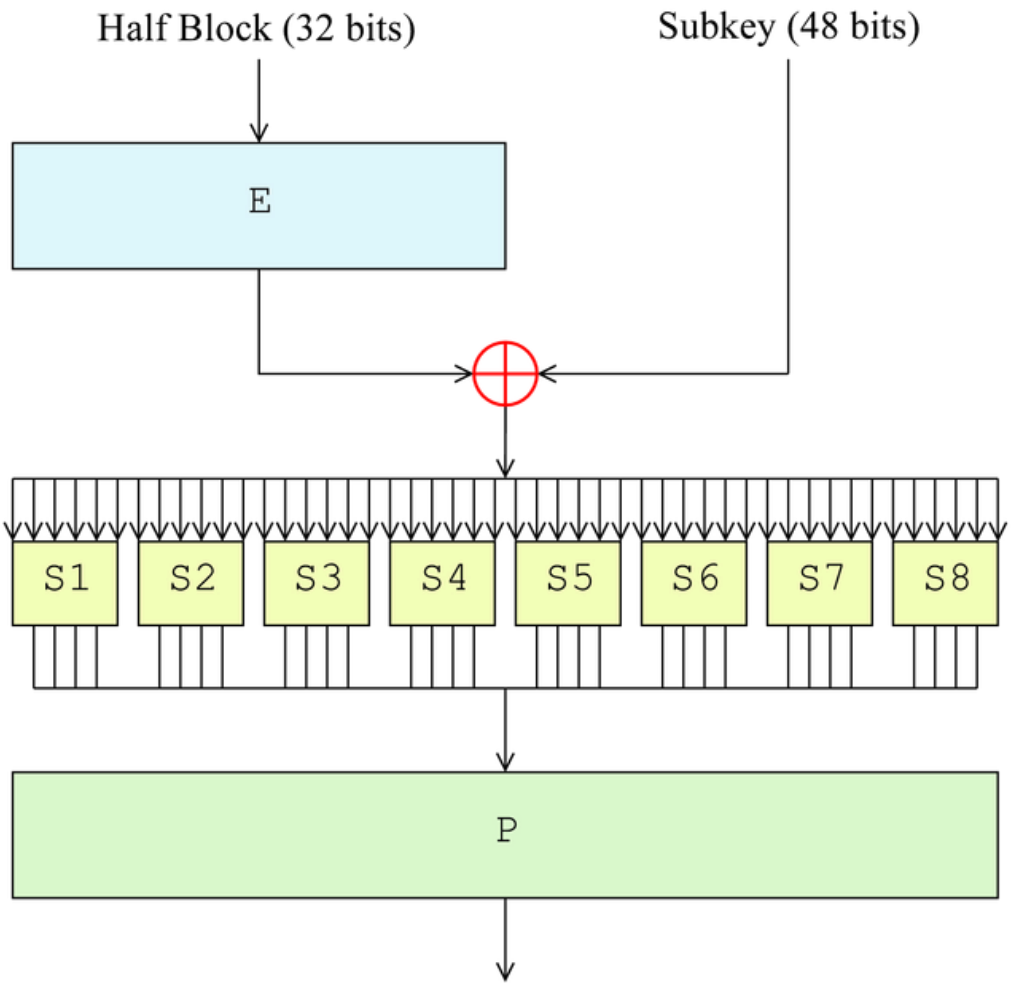
DES simetrik blok şifreleme algoritmasıdır. 1997'de resmi bilgi şifreleme standardı olarak kabul edilirken, 2000'de yerini AES'e bırakmıştır.

DES, büyük boyutlu verilerin şifrelenmesinde kullanılır. Blok şifreleme yöntemi içinde turlar/döngüler kullanılarak şifreli metin ile açık metin arasındaki ilişki azaltılmaya çalışılmaktadır. Her şifreleme adımına döngü denilir ve her döngüde kullanılan anahtar farklıdır. Açık mesaj, belirli uzunluktaki bloklara bölünür ve ayrı ayrı şifrelenen bloklar ile şifreli metin elde edilir. Her bir blok, 8 bit parity biti olmak suretiyle, 64 bit uzunluğundadır. Blok uzunluğu, kullanılan işlemci hızına göre değişebilir. Yeni dönem bilgisayarlarda, 128 bit kullanılmaya başlanmıştır.

DES şifrelemenin en büyük dezavantajı yavaş olmasıdır. Bu yöntemde bilinmezlik fazladır; her bir bloğun her biti, diğer bitler ve anahtar ile bağımlıdır.

DES, bağımlılık fazla olmasına rağmen, modern bilgisayarlara dayanamaz. Brute Force ataklarına karşı güvensizdir. Bu noktada DES'in güvenilirliğini artırmak için 3DES yöntemi geliştirilmiştir. Bu yöntemde, şifrelenen veri farklı anahtar(lar) ile tekrar geri çözülür ve DES şifrelemesi 3 sefer ard arda yapılır (ciphertext = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$) [2] Şifreleme için kullanılan ve uzunluğu 24 byte olan anahtar, 3 bloğa ayrılır. İlk 8 byte ile şifreleme yapılır, buraya kadar olan kısım DES işlemidir. Daha sonra şifrelenen metin ortadaki 8 byte ile çözülür ve son 8 byte ile tekrar şifrelenerek 8 byte'lık blok elde edilir. DES'e göre güvenilirliği fazladır fakat hız 3 kat daha azalmıştır. Her byte bir eşlik biti bulundurur. Dolayısı ile kullanılan anahtar 168 bittir. (24*7=168)

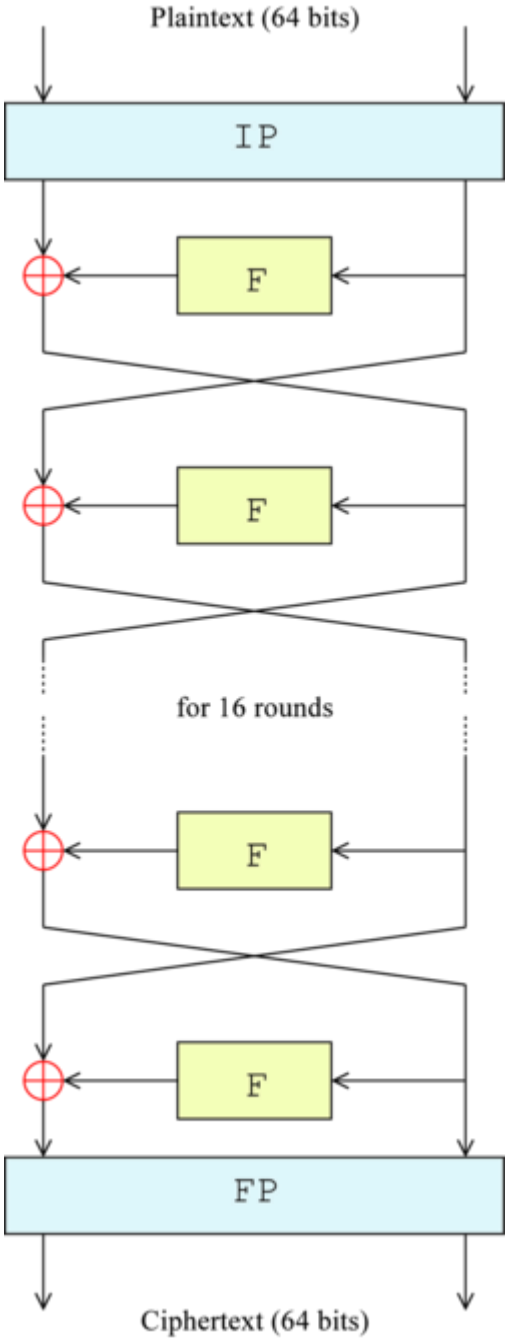
DES'i kırmak için yüksek maliyetle son teknoloji makineler geliştirilmiş olmasına rağmen 3DES, bankalar ve devlet daireleri olmak üzere birçok ortamda kullanılmaya devam etmektedir.



Şekil 1. Feistel (F) Fonksiyonu

DES Algoritması, Feistel fonksiyonlarının ardışık kullanımından oluşmaktadır. Şekil 1 de Feistel algoritması, Şekil 2 de de DES Algoritması gösterilmiştir. Burada amaç, DES algortimasını detaylı olarak anlatmak yerine, DES Algoritmasının genel yapısını anlatmaktır.

DES i güvenli kılan kısmı, lineer olmayan bir transform işlemi olan S-box fonksiyonudur. Şekil 1 de 8 adet S-box (S1 – S8) görülmektedir. Her bir S-box, 6 bitlik datayı alarak 4 bitlik data üretmektedir. S-box fonksiyonunun doğruluk tablosu Şekil 3 de gösterilmiştir.



Şekil 2. DES Algoritması

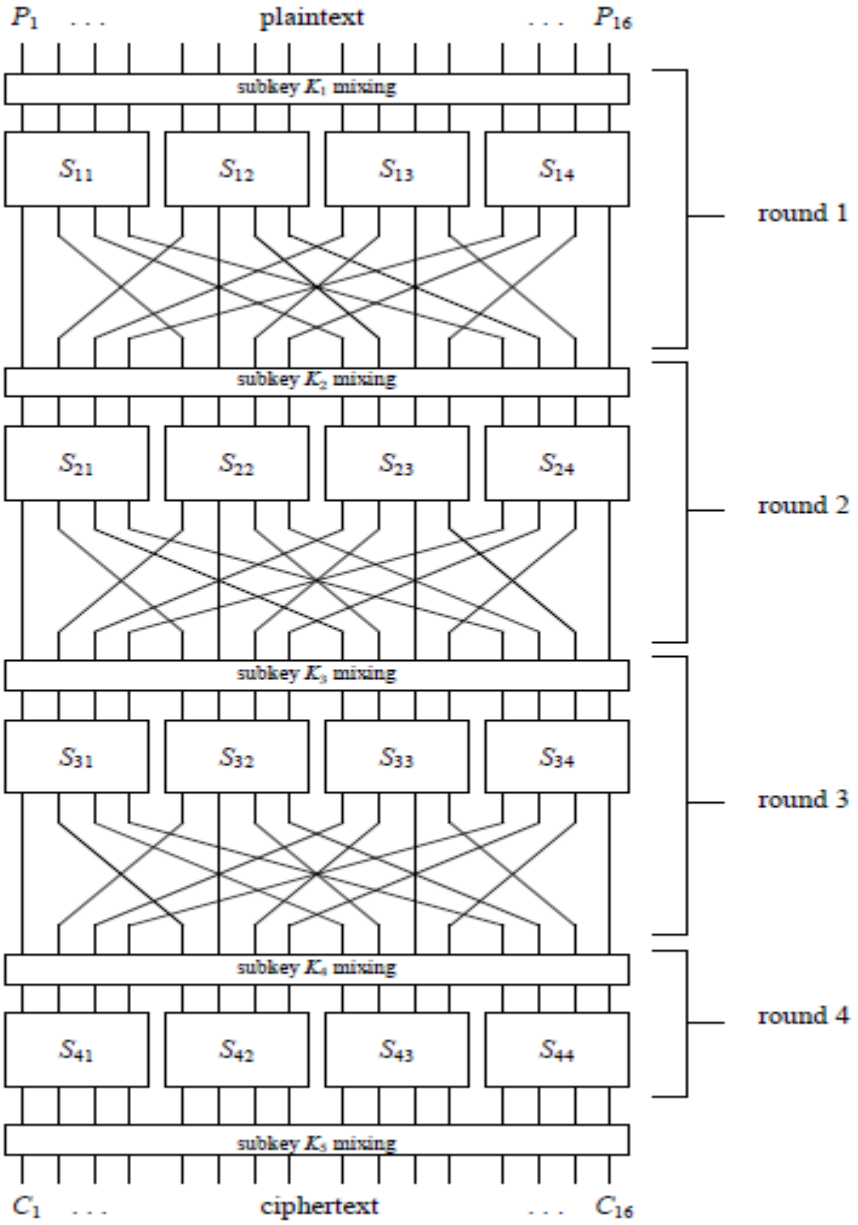
S_5		Orta 4 bit															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
İlk ve son bitler	**00**	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Şekil 3. 6x4 bitlik S-box

Örnek olarak, S-box fonksiyonuna input olarak 011011 verirsek, ilk ve son bit 01 olacak, orta 4 bit de 1101 olacaktır. Sonuç, 1001 olur.

3. BASİT ŞİFRELEME YÖNTEMİ

Kullanacağımız şifreleme yöntemi, DES e benzer şekilde dizayn edilmiş, temel Yerine Koyma-Permütasyon Ağı fikrine dayalı bir yöntemdir. Bu yöntem, Şekil 4 de gösterilmiştir. Şekilde 4 roundluk bir algoritma gösterilmiş olmakla beraber, biz lineer kriptanaliz için 2 roundluk bir algoritma kullanacağız. Bu SPN ağında 16 bitlik açık metin 4 er bitlik bloklara ayrılıp S-Box adı verilen yerine koyma bloklarına gönderilir. Bu bloklar doğrusal olmayan şekilde çalıştıkları için Asıl güvenli olan kısım burasıdır. Şekil 3de bu S-BOX ların çalışmasına bir örnek verilmiştir.



Şekil 4. Kullanacağımız Basit şifreleme yönteminin 4-round hali.

Her döngü (round), 3 işlemden oluşmaktadır:

- Yerine Koyma: Burada yerine koyma fonksiyonu, şekilde S harfi ile gösterilmiştir. Yerine koyma işlemi, Tablo 1 de gösterilmiştir.

input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
output	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Tablo 1. Yerine Koyma Fonksiyonu (hexadecimal olarak gösterilmiştir).

- Permütasyon: Permütasyon işlemi, eldeki verinin bitlerinin basit bir şekilde yer değiştirmesidir. Kullandığımız şifreleme algoritmasındaki permütasyon işlemi, Tablo 2 de gösterilmiştir. Örnek olarak, 10. sıradaki bitin yeri değiştirilerek 7. sıraya yazılacaktır.

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

Tablo 2. Permütasyon Fonksiyonu (hexadecimal olarak gösterilmiştir).

- Anahtar Ekleme: Anahtar ekleme işlemi, basit bir XOR işlemidir. Round anahtarı, şekil 4 de gösterildiği gibi, permütasyon işleminden geçmiş data ile XOR lanacaktır.

Şifre çözme işlemi, şifreleme algoritmasında uygulanan işlemlerin tam tersi uygulanarak yapılır.

LİNEER KRİPTANALİZ

Lineer kriptanaliz; düz metin, şifreli metin ve döngü anahtarlarının bitleri kullanılarak oluşturulan lineer denklemlerin bazılarının yüksek olasılıkla doğru olmasını kullanılarak yapılan atak şeklidir. Atak yapan kişinin elinde düz metin-şifreli metin çiftlerinin olması durumunda yapılabilen bir ataktır. Ancak, atak yapan kişi, istediği düz metin-şifreli metin çiftini oluşturamaz. Dolayısıyla bu çiftlerin rastgele bilgiler olduğu varsayılır.

Buradaki temel fikir şudur: şifreleme yapılırken kullanılan herhangi bir denklemi, lineer olan başka bir denklem şeklinde yazmaktır. Bahsedilen bu lineer denklem şu şekildedir:

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

Burada X_i, işlemin girdisi olan X in i. bitini, Y_j de işlemin çıktısı olan Y nin j. bitini ifade etmektedir. Bu eşitlik, u girdi bitinin ve v çıktı bitinin birbiriyle XOR lanmasını göstermektedir.

Lineer kriptanalizde amaç, yukarıda açıklanan biçimde denklemler yazarak, bu denklemlerin yüksek veya düşük olasılıkla doğru olanlarını belirlemektir. Eğer bir şifreleme yönteminde yukarıdaki şekilde olan ve yüksek veya düşük olasılıkla doğru olan denklemler bulabilirsek, bu bize bu şifreleme yönteminin zayıflığını gösterir. Mükemmel bir şifreleme algoritması olsaydı, yukarıdaki şekilde yazılabilecek herhangi bir denklemin doğru olma olasılığı ½ olurdu. Lineer kriptanaliz, ½ olasılığından sapmaları inceleyerek bu sapmaları kullanmaya çalışmaktadır. Bu sapmalara doğrusal olasılık sapması (linear probability bias) denir ve $p_L > ½$ veya $p_L < ½$ olması linear kripto analiz için eşit derecede etkilidir. Bu açıklık SPN ağındaki tek doğrusal olmayan kısım olan S-Box (yerine koyma) blokları düşünülerek yapılacaktır. Bir kere S-Box ların giriş ve çıkışları arasında doğrusal yaklaşımlar ifade edilebilirse ve sonradan bu ifadeler birbirlerine eklenip en sonunda tüm sistem için doğrusal bir ifade elde edilebilir. Bu işin temelinde Yığma prensibi (piling up Lemma) kullanılmaktadır. O yüzden ilk önce yığma prensibi üzerinde durulacaktır.

Yığma Prensibi

Elimizde iki rastgele ikili değişken olduğunu varsayalım, bunlar da X_1 ve X_2 olsun. $X_1 \oplus X_2 = 0$ lineer denkleminin doğruluk tablosunu oluşturalım. Burada, X_1 ve X_2 nin olasılık dağılımı aşağıdaki gibi ise:

$$\Pr(X_1 = i) = \begin{cases} p_1 & ,i = 0 \\ 1 - p_1 & ,i = 1 \end{cases}$$

$$\Pr(X_2 = i) = \begin{cases} p_2 & ,i = 0 \\ 1 - p_2 & ,i = 1. \end{cases}$$

ve iki değişken birbirinden bağımsız ise:

$$\Pr(X_1 = i, X_2 = j) = \begin{cases} p_1 p_2 & ,i = 0, j = 0 \\ p_1(1-p_2) & ,i = 0, j = 1 \\ (1-p_1)p_2 & ,i = 1, j = 0 \\ (1-p_1)(1-p_2) & ,i = 1, j = 1 \end{cases}$$

ve buradan şunu çıkarabiliriz:

$$\begin{aligned} \Pr(X_1 \oplus X_2 = 0) &= \Pr(X_1 = X_2) \\ &= \Pr(X_1 = 0, X_2 = 0) + \Pr(X_1 = 1, X_2 = 1) \\ &= p_1 p_2 + (1-p_1)(1-p_2). \end{aligned}$$

Burada $p_1 = ½ + \varepsilon_1$ ve $p_2 = ½ + \varepsilon_2$ şeklinde yazarsak,

$$\Pr(X_1 \oplus X_2 = 0) = 1/2 + 2\varepsilon_1\varepsilon_2 \qquad (2)$$

olur. Buradaki $X1 \oplus X2 = 0$ ın sapması (bias) $2\varepsilon_1\varepsilon_2$ dir.

Burada iki bit için yapılan işlem n adet bit için yapıldığı düşünürse X_1 den X_n e olasılıkları $p_1=1/2 - \varepsilon_1$ den $p_n=1/2-\varepsilon_n$ için, birbirinden bağımsız olan n adet bit için Pilling-Up Lemma

$$\Pr(X_1 \oplus \ldots \oplus X_n = 0) = 1/2 + 2^{n-1}\prod_{i=1}^{n}\varepsilon_i$$

yada

$$\varepsilon_{1,2,..,n} = 2^{n-1}\prod_{i=1}^{n}\varepsilon_i \qquad (3)$$

$\varepsilon_{1,2,\ldots,n}$ $X_1 \oplus X_2 \oplus \ldots\ldots X_n = 0$ ın sapması (bias) ını göstermektedir.

Şifreli sistemin doğrusal yaklaşımını geliştirmek için, Xi değerleri aslında S-Box ın doğrusal bir yaklaşımını temsil edeceklerdir. Örneğin 4 birbirinden bağımsız rastgele ikili değişkeni düşünelim X1, X2, X3, ve X4. $\Pr(X_1 \oplus X_2 = 0) = 1/2 + \varepsilon_{1,2}$ ve $\Pr(X_2 \oplus X_3 = 0) = 1/2 + \varepsilon_{2,3}$ olsun, $X_1 \oplus X_3$ toplamının $X_1 \oplus X_2$ $X_3 \oplus X_2$ den elde edileceğini düşünün. Bu şekilde

$$\Pr(X_3 \oplus X_1 = 0) = \Pr([X_1 \oplus X_2] \oplus [X_2 \oplus X_3] = 0) \qquad (4)$$

Bu şekilde yeni bir doğrusal ifade oluşturmak için iki doğrusal ifadeyi birleştiriyoruz. $X_1 \oplus X_2$ ve $X_2 \oplus X_3$ rastgele değerlerini birbirinden bağımsız olarak değerlendirebileceğimiz için Pilling up Lemma (yığma prensibini) kullanarak aşağıdaki sapmayı (bias) yazılabilir.

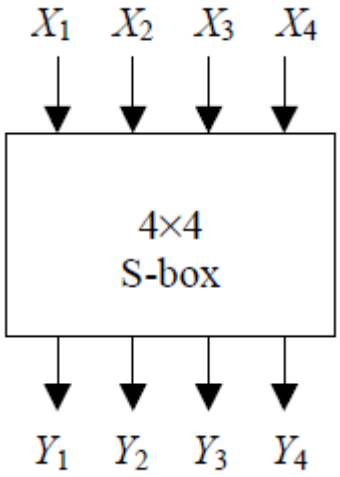
$$\Pr(X_1 \oplus X_3 = 0) =) = 1/2 + 2\varepsilon_{1,2}\,\varepsilon_{2,3}$$

$$\varepsilon_{1,3} = 2\varepsilon_{1,2}\,\varepsilon_{2,3} \qquad (5)$$

Anlaşılacağı gibi $X_1 \oplus X_2 = 0$ ve $X_2 \oplus X_3 = 0$ S-Boxların doğrusal yaklaşımına benzemekteyken, $X_1 \oplus X_3 = 0$ da ara durum olan X2 nin elimine edildiği bir şifreme sistemine benzemektedir. Elbette gerçek sistemde çok daha karmaşık olan S-Box çıkışlarını benzetilmesi gerekli olacaktır.

S-Box Analizi

Bir saldırı başlatılmadan önce S-Box lardaki doğrusal açıklıkların varlığını tespit edilmesi gereklidir. Giriş $X=[X_1\ X_2\ X_3\ X_4]$ ve karşılık çıkışları $Y=[Y_1\ Y_2\ Y_3\ Y_4]$ dikkate alındığında tüm doğrusal yaklaşımların sapmaları incelenir.



Şekil 5 X girişlerine karşılı Y çıkışlarını gösteren S-Box görüntüsü

$$X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4 . \tag{6}$$

Örneğin denklem 6 daki denklem düşünüldüğünde, lineer denklemini, X in bütün olası değerleri için incelersek, 16 durumdan 12 sinde doğru olduğunu görürüz. Yani bu denklemin doğruluk oranı 12/16 - ½ = ¼ olur. Bu Tablo 3 den de gözükmektedir.

Benzer şekilde Tablo 3 incelediğinde $X_1 \oplus X_4 = Y_2$ için sapma olasılığının 0 iken, $X_3 \oplus X_4 = Y_1 \oplus Y_4$ sapması 2/16-1/2= -3/8 olacaktır.

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$	$X_1 \oplus X_4$	Y_2	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
1	0	0	0	0	0	1	1	0	0	1	0	0	1
1	0	0	1	1	0	1	0	0	0	0	0	1	1
1	0	1	0	0	1	1	0	1	1	1	1	1	0
1	0	1	1	1	1	0	0	1	1	0	1	0	1
1	1	0	0	0	1	0	1	1	1	1	1	0	1
1	1	0	1	1	0	0	1	1	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	1	0	1	0
1	1	1	1	0	1	1	1	0	0	0	1	0	1

Tablo 3 S-Box kutusu için Örnek Lineer yaklaşım

X ve Y değerlerinin olası bütün lineer denklem kombinasyon denklemlerini incelersek, aşağıdaki Tablo 4 ü elde ederiz. Tablodaki her sayı, girişlerin toplamı olarak ifade edilen doğrusal denklem ile, çıkışların toplamı olarak ifade edilen doğrusal denklem Eşitlik durumlarının 8 den çıkarılmış halini göstermektedir.

		Output Sum															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Input Sum	0	+8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	–2	–2	0	0	–2	+6	+2	+2	0	0	+2	+2	0	0
	2	0	0	–2	–2	0	0	–2	–2	0	0	+2	+2	0	0	–6	+2
	3	0	0	0	0	0	0	0	0	+2	–6	–2	–2	+2	+2	–2	–2
	4	0	+2	0	–2	–2	–4	–2	0	0	–2	0	+2	+2	–4	+2	0
	5	0	–2	–2	0	–2	0	+4	+2	–2	0	–4	+2	0	–2	–2	0
	6	0	+2	–2	+4	+2	0	0	+2	0	–2	+2	+4	–2	0	0	–2
	7	0	–2	0	+2	+2	–4	+2	0	–2	0	+2	0	+4	+2	0	+2
	8	0	0	0	0	0	0	0	0	–2	+2	+2	–2	+2	–2	–2	–6
	9	0	0	–2	–2	0	0	–2	–2	–4	0	–2	+2	0	+4	+2	–2
	A	0	+4	–2	+2	–4	0	+2	–2	+2	+2	0	0	+2	+2	0	0
	B	0	+4	0	–4	+4	0	+4	0	0	0	0	0	0	0	0	0
	C	0	–2	+4	–2	–2	0	+2	0	+2	0	+2	+4	0	+2	0	–2
	D	0	+2	+2	0	–2	+4	0	+2	–4	–2	+2	0	+2	0	0	+2
	E	0	+2	+2	0	–2	–4	0	+2	–2	0	0	–2	–4	+2	–2	0
	F	0	–2	–4	–2	–2	0	+2	0	0	–2	+4	–2	–2	0	+2	0

Tablo 4 Doğrusal Yaklaşım Tablosu

Bu deneyde sizden istenen, yukarıdaki lineer tahmin tablosunu hesaplayıp ekrana basmanızdır.

Tüm Şifreleme Sistemi için Doğrusal yaklaşımın oluşturulması

S-Boxlar için doğrusal yaklaşım yapıldıktan sonra komple sistem için bir doğrusal yaklaşım hazırlanmak kolaylaşacaktır. Bu bölümde olası bir sistem için komple sistem doğrusal yaklaşımının nasıl yapılacağı bir örnek üzerinden anlatılmaya çalışılacaktır. Daha önceden de ifade edildiği gibi giriş bitleri ve çıkış bitleri arasında oluşturulacak doğrusal bir denklem ara anahtarların bir kısım bitlerine erişmek için bilgi verecektir.

Bunun için Şekil 4 deki gibi sistemin 4 turluk olduğu kabul edelim ve S_{12}, S_{22}, S_{32}, S_{34} deki doğrusal yaklaşım denklemleri aşağıdaki gibi olsun

$S_{12}: X_1 \oplus X_3 \oplus X_4 = Y_2$ 12/16 olasılık ve +1/4 sapma ile (7)

$S_{22}: X_2 = Y_2 \oplus Y_4$ 4/16 olasılık ve sapma -1/4 (8)

$S_{32}: X_2 = Y_2 \oplus Y_4$ 4/16 olasılık ve sapma -1/4 (9)

$S_{34}: X_2 = Y_2 \oplus Y_4$ 4/16 olasılık ve sapma -1/4 (10)

Tüm sistemi tek bir doğrusal denklemde ifade edebilmek ve S-Box giriş ve çıkışlarında kullanılan notasyonun karışmaması için giriş ve Çıkışlar X ve Y yerine U ve V olarak ifade edilirken alt simgelerde U_i ve V_i 16 bit giriş ve çıkışı temsil ederken i tur u ifade edecektir. Ui, j ve Vi, j ise i. Turdaki j. bitini temsil edecektir. Bitler soldan başlayarak 1 den 16 kadar numaralandırılmıştır. Ki, j i. turda kullanılan alt anahtarın j. bitini temsil etmektedir.

U1 turun çıkışı P sade metnin K1 anahtarı ile EXor işlemine tabi tutulmasıdır. $U_1 = K_1 \oplus P$. Denklem (7) kullanılarak denklem 11 elde edilebilir.

$$\begin{aligned} V_{1,6} &= U_{1,5} \oplus U_{1,7} \oplus U_{1,8} \\ &= (P_5 \oplus K_{1,5}) \oplus (P_7 \oplus K_{1,7}) \oplus (P_8 \oplus K_{1,8}) \end{aligned} \quad (11)$$

11 in olasılık oranı 3/4 dür. İkinci turdaki yaklaşım için elimizde denklem 12 mevcuttur. Denklem (8) den elde edilmiştir.

$$V_{2,6} \oplus V_{2,8} = U_{2,6} \tag{12}$$

12 nin olasılık oranı 1/4 dür. $U_{2,6} = V_{1,6} \oplus K_{2,6}$, olduğu için denklem 13 elde edilebilir.

$$V_{2,6} \oplus V_{2,8} = V_{1,6} \oplus K_{2,6} \tag{13}$$

13 un olasılık oranı ¼ olacaktır. Olasılık oranı 3/4 olan Denklem 11 ile birleştirildiğinde elimizde denklem 14 deki gibi yazılabilir.

$$V_{2,6} \oplus V_{2,8} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} = 0 \tag{14}$$

Buda 1/2 + 2(3/4-1/2)(1/4-1/2)=3/8 olasılığa sahip olacaktır bunun sapma oranı ise -1/8 olacaktır (Pilling Up Prensipi kullanıldığında) . Burada SBOx ların birbirinden bağımsız olduğunu kabul ediyoruz ki bu her zaman olması gerekli bir durum değildir.

3. tur için olasılığı 1/4 olan

$$V_{3,6} \oplus V_{3,8} = U_{3,6} \tag{15}$$

ve olasılığı 1/4 olan

$$V_{3,14} \oplus V_{3,16} = U_{3,14} \tag{16}$$

$U_{3,6} = V_{2,6} \oplus K_{3,6}$ ve $U_{3,14} = V_{2,8} \oplus K_{3,14}$ olduğu için denklem 17 elde edilebilir.

$$V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus V_{2,6} \oplus K_{3,6} \oplus V_{2,8} \oplus K_{3,14} = 0 \tag{17}$$

denklem 17 nın olasılığı $1/2+2(1/4-1/2)^2 = 5/8$ ve +1/8 sapması vardır. Gene Piling Up prensibi kullanılarak 14 ve 17 nolu denklemler birleştirildiğinde denklem 18 elde edilecektir

$$V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} = 0. \tag{18}$$

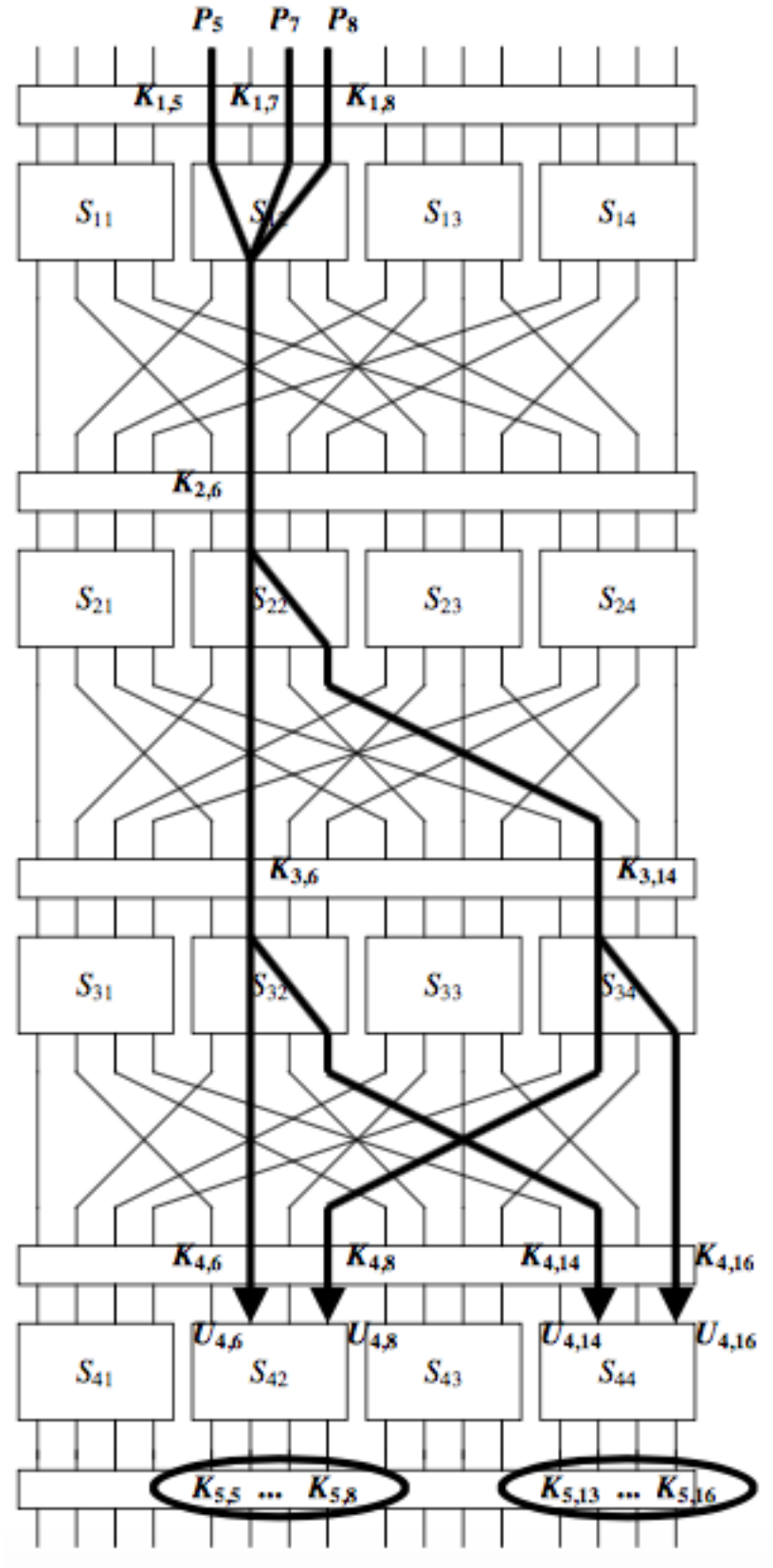
$U_{4,6} = V_{3,6} \oplus K_{4,6}$, $U_{4,8} = V_{3,14} \oplus K_{4,8}$, $U_{4,14} = V_{3,8} \oplus K_{4,14}$, nın ve $U_{4,16} = V_{3,16} \oplus K_{4,16}$ şeklinde ifade edilebileceğinden denklem 19 yazılabilir.

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus \Sigma_K = 0. \tag{19}$$

$$\Sigma_K = K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} \oplus K_{4,6} \oplus K_{4,8} \oplus K_{4,14} \oplus K_{4,16}$$

Piling up Lemma kullanılarak denklem (19) un olasılığının $1/2 + 2^3(3/4-1/2)(1/4-1/2)^3=15/32$ ve -1/32 sapma ya sahiptir. Σ_K 0 yada 1 olacaktır ve bu şekilde sabit kabul edildiğinde denklem 20 elde edilir.

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 = 0 \tag{20}$$



Şekil 6 Doğrusal denklem çıkarılırken izlenen yollar

Anahtarları Çıkarma

R-1 inci turun sonundaki doğrusal denklemi elde etmek anahtarları çözmek için yeterli K5 in bitlerini ayırmak mümkün olacaktır. Bulunan Doğrusal denklemden etkilene son tura ait S-Boxlarla ExOr işlemine sokulan K5

anahtarına ait bitler Tahmin için hedef seçilen bitler olacaktır. Daha önceden elde edilmiş çok sayıda açık metin şifreli metin çiftinden yararlanılarak en son Tur 3. Tur a kadar tahmin edilen Anahtar bitleri ile kısmi olarak deşifre edilir. Her bir anahtar tahmin değerine bir sayaç ilişkilendirilir ve sayaç bilinen sade metin şifrelenmesi ile hesaplanan doğrusal denklem üzerinden örtüşüyorsa değeri 1 arttırılır. Doğru tahmin edilmiş hedef bitlerin olasılığı daha ½ den oldukça uçak olacaktır. Bu şekilde kısmı olarak bitler bulunduktan son diğer bitlerde açığa çıkarılır.

$$| \text{bias} | = | \text{count} - 5000 | / 10000$$

partial subkey $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	| bias |	*partial subkey* $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	| bias |
1 C	0.0031	2 A	0.0044
1 D	0.0078	2 B	0.0186
1 E	0.0071	2 C	0.0094
1 F	0.0170	2 D	0.0053
2 0	0.0025	2 E	0.0062
2 1	0.0220	2 F	0.0133
2 2	0.0211	3 0	0.0027
2 3	0.0064	3 1	0.0050
2 4	**0.0336**	3 2	0.0075
2 5	0.0106	3 3	0.0162
2 6	0.0096	3 4	0.0218
2 7	0.0074	3 5	0.0052
2 8	0.0224	3 6	0.0056
2 9	0.0054	3 7	0.0048

1/32 = 0.03125 e en yakın seçilen anahtara alt seti uygun anahtar olarak belirlenir.

Bu Laboratuvar notlarının büyük kısmı Howard M. Heys in ***A Tutorial on Linear and Differential Cryptanalysis*** adlı çalışmasından yararlanılarak hazırlanmıştır.

Referenslar

[1] M. Matsui, "Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology- EUROCRYPT '93 (Lecture Notes in Computer Science no. 765), Springer-Verlag, pp. 386-397, 1994

[2] "Triple DES", http://en.wikipedia.org/wiki/Triple_DES 3.11.2014 erişim tarihi

[3] Howard M. Heys, ***Tutorial on Linear and Differential Cryptanalysis***
http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf