BÖLÜM 8

KRİPTANALİZ

Kriptanaliz (Kripto-analiz) bölümünde modern kripto sistemleri içerisinde önemli bir sınıf teşkil eden simetrik anahtarlı sistemler olarak bilinen blok şifrelerin ve akan şifrelerin analizi görülecektir. ***Kerckhoff's prensibi*** : Kripto-analizci şifreleme algoritmasının bütün detaylarına ulaşma gücüne sahiptir ve sistemde sadece anahtar gizlidir.

Bu prensibe göre tasarlanmış ve hala güvenli olduğu kabul edilen birçok algoritma günümüzde mevcuttur.

İkinci Dünya Savaşında Polonyalı ve İngiliz matematikçiler Alman Enigma şifreleme makinasının analizini yaparak algoritmayı kırmışlardır ve Alman kapalı metinlerini kripto-analiz yöntemi ile açmışlardır. Farklı bir algoritma olan ve belli bir süre güvenli olarak kabul edilmiş olan RC4 algoritması "tersine giderek" (reverse engineering) ile kırılmıştır.

- Analizcinin amacı herhangi bir algoritma kullanılarak kapatılmış metinlerin açık halini elde edebilmektir. Genellikle bu amaca algoritmada kullanılan gizli anahtarın tamamı veya belli bir kısmı elde edilerek ulaşılır.
- Analiz yönteminin ne kadar kuvvetli ve efektif olduğu analiz için gerekli olan önbilgi ve yapılacak iş miktarı ile ölçülür (bilinmesi gerekenler açık-kapalı metin çiftlerinin sayısı, harcanan zaman, atağın başarı oranı dır).

Atak Çeşitleri (Senaryoları) :

- **Sadece Şifreli Metin Atağı** (Ciphertext-Only) : En güçlü kripto-analitik atakdır. Sadece haberleşme pasif olarak dinlenip (müdahale edilmeden)yeterince kapalı metin elde edilerek yapılabilir.
- **Bilinen Açık Metin Atağı** (Known Plaintext): Bir miktar açık-kapalı metin çifti bilinerek yapılan ataktır. Mesajların bir kısmı tahmin edilebilir veya açık gönderilen mesajlar toplanarak atak uygulanabilir.
- **Seçilmiş Açık Metin Atağı** (Chosen Plaintext): Analizcinin istediği (seçtiği) metni şifreleme imkanına sahip olduğu kabul edilen atak senaryosudur. Analizci şifreleme algoritmasının güvenli olarak yerleştirildiği mekanizmayı elde edebilir. Analizci aktif olarak haberleşme sisteminde rol alır.
- **Seçilmiş Kapalı Metin Atağı** (Chosen Ciphertext): Deşifreleme makinasına ulaşılarak yapılan atak çeşitidir. Bir önceki senaryoya benzemektedir.
- **Seçilmiş Açık veya Kapalı Metin Atağı** (Adaptive Chosen Plaintext or Ciphertext): Bu atak senaryosunda analizcinin istediği mesajı açma veya kapatma konusunda sınırsız kapasiteye sahip olduğu kabul edilir. Önceki iki senaryonun teorik olarak daha güçlendirildiği atak çeşitidir.

8.1 Kriptanalitik Atakların Amaçları

Ayıran Ataklar (Distinguishing Attacks) Ayıran Atakların başarılı olabilmesi için şifre sisteminin çıktısını rastgele bir permutasyonun çıktısından ayırılaması olası olmalıdır.

Kısmi açık metin bilgisi (Partial Knowledge of the Plaintext) Bu atakta kısmi açık metin bilgisine (Şifre sisteminin girdisi için herhangi tahmin) sahip olunur.

Deşifreleme (Decryption) Bu durumda saldıran şifrelenmiş trafiğin bir kısmını deşifre etme yeteneğine sahiptir.

Şifreleme (Encryption(Forgery))

Bu durumda saldıran anlamlı mesajları bilinmeyen gizli anahtar ile şifreleme olanağına sahiptir. Bu gizli anahtar bilgisine sahip olduğu anlamına gelmez. Bu atağa meyilli olan şifre sistemleri gerçekliğini **kanıtlama/kimlik belirtme** işlemlerinde kullanım için uygun değillerdir.

Kısmı Anahtar Edinimi (Partial Key Recovery) Bu atakta gizli anahtarın belli bir kısmı saldıran tarafından ele geçirilir. Belki bu anahtarın geriye kalan kısmı çok büyük olabilir fakat bu arzulanan bir durum değildir. Çünkü tüm anahtarın genellikle ele geçirilmesi için ilk basamaktır.

Tüm Anahtar Edinimi (Total Key Recovery) Bir kriptosistem için en korkunç kriptanalitik atak çeşidir.

8.2 Kriptanaliz Metodları(Methods of Cryptanalysis)

Eğer şifre sistemi temiz ve basit bir yapıya sahip ise hala kalem ve kağıt kriptanalistin elindeki en güçlü silahlardır. Bir çok durumda kağıt analizi bilgisayar analizinden gelen geribildirimlere (özel istatiksel özellikler ve düzensizlikler arama gibi) ihtiyaç duyar. Araştırmacı bakış açısından bir şifre sistemi kırıldığının dile getirilmesi, bu sistemin dizaynı değiştirmeye yol açacak bir zayıflığının bulunması demektir. Bu değişiklik, ek döngülerin eklenmesi veya döngü anahtarlarını oluşturan algoritmanın ve bazı iç yapıların değişmesi anlamına gelebilir. Şifre sisteminin tamamen kırılması ise bu tür sistemi tamir etmek yerine baştan tasarlamanın daha anlamlı veya kolay olduğu durumlardır. Tipik kriptanaliz metodlarını şöyle sıralayabiliriz:

Etraflı Arama (Exhaustive Search) Etraflı Arama, şifre sistemleri üzerine en açık ve en doğrudan uygulanabilir bir methodur. Tüm olası gizli anahtarları bilinen kısa açık/kapalı metin örnekleri üzerinde dener. Doğru gizli anahtar bilinen açık bir metinden doğru kapalı metinin elde edilmesini sağlar. Günümüz hesaplama imkanlarına göre modern blok şifre sistemlerinin anahtar uzunlukları (128-bit ve yukarısı) bu tip atağı imkansız kılacak şekilde seçilmektedir. DES in en önemli zayıflığı 56-bit olan kısa anahtar uzunluğudur ve günümüz koşulları düşünüldüğünde bu anahatar uzunluğu etraflı aramayı mümkün kılmaktadır.

Sözlük Atakları (Dictionary Attacks)

Bu da basit fakat blok şifre sistemleri için önemli bir atak çeşidir. Eğer şifrelenen metinlerin uzunlukları kısa ise saldıran birçok metin toplar ve farklı metinlerin tekrar-

lama analizini yapar. En uç noktada bu atağa zayıf şifre sistemi basit değiştirmeli şifre sistemidir (simple substitution cipher).

Eş Tanımlama (Equivalent Description)

Bazen şifre sistemi tasarlayanlar sistemin veya parçalarının basit eşdeğer tanımlarını gözden kaçırırmaları, bu atak tarafından sömürülür.

Değişmezler için Devirlilik veya Arama (Periodicity or Search for Invariants) Değişmezler, şifreleme boyunca değişmeyen özellikler olarak düşünelebilir ve şifre sisteminin istenilmeyen bir özelliğidir. Eğer kriptanalist sistemin herhangi değişmezini yada yakınsamasını bulmayı başarırsa bir ayıran atak için malzeme edinmiş olur. Her çeşit devirli davranış veya şifrelenmeler arasındaki korelasyon mutlaka engelllemelidir.

Doğum Günü Paradoks (Birthday Paradox) Blok şifreleme sistemlerinden açık anahtar şifre sistemlerine uzunan sayılamıyacak kadar önemli bir olasılıklı paradoksudur.

Ortada buluşma Atağı (Meet-in-the-Middle Attack) Bu metod şifreleme sistemini alt ve üst olmak üzere böler. Sonra kısmi tahmini ile yukarıdan ortaya ve baştan ortaya kısmi deşifreleme yapar. Sonuç karşılaştırılır ve eğer uyumlu ise aday anahtar saklanır. Aksi takdirde tahmin edilen anahtar yanlış olur.

İstatiksel Yaklaşımlar (Statistic Approaches)

Bu metodlar kapalı ve açık metin arası ilişki veren istatiksel örnekleri arar. Bir tür ayıran ataktır ve diğer ataklar için ilk adımdır. İstatiksel yaklaşımlar hem oluşması yüksek olasılıkta olayları hem de gerçekleşmesi imkansız olayları bulmaya yöneliktir.

Özel bir Atağa göre Zayıf Anahtarlar (Weak Keys with Respect to a Particular Attack)

Bazı durumlarda bir zayıf anahtar kümesinin bir şifre sisteminin analizini özel bir atak modelini düşünüldüğünde kolaylaştırması mümkün olmaktadır. Eğer bir kriptosistemin tüm anahtar uzayına göre yüksek bir oranda zayıf anahtarlara sahip ise tekrar dizayn edilmesi bile söz konusu olabilir.

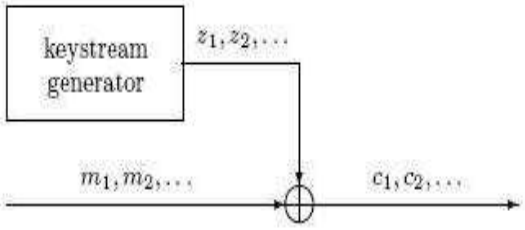
Örnek olarak DES te dört tane zayıf ve oniki tane yarı-zayıf anahtar bulunmaktadır. Gizli anahtar K olmak üzere DES i E_K olarak tanımlarsak dört tane zayıf anahtar için $E_K(E_K(m)) = m$ ve oniki tane yarı-zayıf anahtardan iki tanesi için $E_{K1}(E_{K2}(m)) = m$ sağlanmaktadır. IDEA blok şifre sistemi için 2^{128} anahtar uzayı üzerinde 2^{63} elemana sahip bir zayıf anahtar kümesi bulunmaktadır.

8.3 Akan Şifrelerin Analizi

İyi bir akan şifre algoritması bilinen açık metin atağa karşı dayanıklı olmalıdır. Genel olarak akan şifrelerin oluşturulmasında temel yapı taşları olarak LFSR'lar kullanılır ve gizli anahtar (secret key) LFSR'ların başlangıç konumları olarak (initial state) seçilir. Akan şifrelerin analizinde korelasyon atağı şu şekildedir.

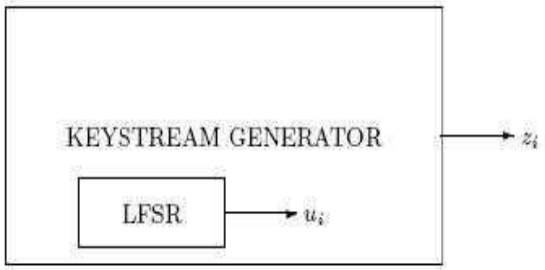
Akan şifrelerde anahtar üreticinin kullanımı

$c_i = m_i \oplus z_i \;\Rightarrow\; z_i = c_i \oplus m_i$



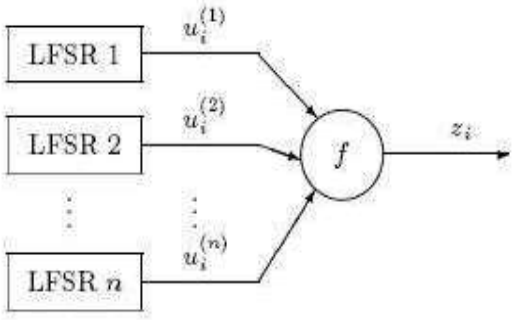
Bilinen açık metin atağı: Belirli açık-kapalı mesaj çiftleri (m_i, c_i), z_i'ler bilinirken gizli anahtarı bulabilmektir.

Korelasyon atağı için gerekli ve yeterli koşul $u_i = z_i$ olma olasılığının 0.5 den farklı olmasıdır. Eğer$P$ olasılığı gösterirse, bunu matematiksel olarak $P(u_i = z_i) \neq 0.5$ şeklinde ifade edebiliriz.

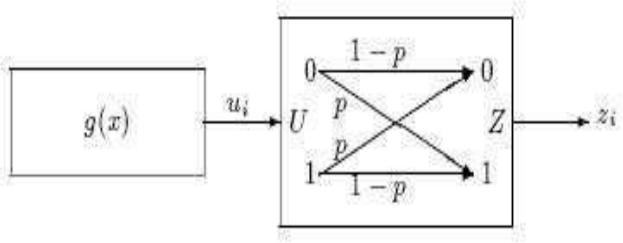


Korelasyon atak için gerek ve yeter şart $P(u_i = z_i) \neq 0.5$

Nonlinear (Doğrusal Olmayan) fonksiyonlarla LFSR'ları birleştirme (prensibi)



Eğer f fonksiyonu $(m-1)$-dayanıklı (m-dayanıklı olmayan) bir fonksiyonsa $P(z_i = u_i^{(a_1)} + u_i^{(a_2)} + \cdots + u_i^{(a_m)}) \neq 0.5$ dir. Bu durumda f'nin korelasyon atağına dayanıklı olması için m değerinin yeterince yüksek olması gereklidir.



Korelasyon atak Modeli

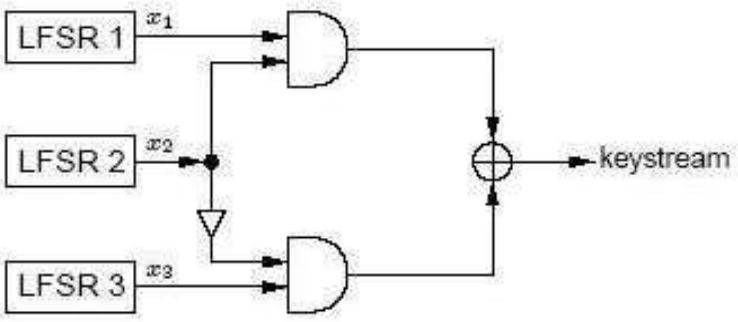
Yukarıdaki sistemde korelasyon ihtimali $1 - p = P(u_i = z_i)$ ve hata ihtimali p'dir.

Korelasyon Atağı: Resim 4 deki sistemde bütün LFSR'ların maksimum periyoda sahip olduğunu kabul edelim ve LFSR'ların uzunluklarını $L_1, L_2, \ldots, L_n$ ile gösterelim. Eğer bu

sistemdeki LFSR'ların bağlantı polinomları ve f fonksiyonu biliniyorsa en fazla $\prod_{i=1}^{n}(2^{L_i}-1)$ adet farklı anahtar üretilebilir. Üretilen anahtar dizisi ile herhangi bir LFSR'ın - buna R_1 diyelim; çıktısı arasındaki korelasyon ihtimali $p > 0.5$ veya $(p < 0.5)$ ise ve anahtar dizisinin yeterince uzun kısmı biliniyorsa R_1'in başlangıç konumu bilinen anahtar dizisi ile R_1'in çıktısının bütün olası kaydırılmış halleri arasındaki çakışmaların sayısı ile bulunabilir. Çakışma sayısının korelasyon ihtimali ile tutması gereklidir. Bu durumda R_1'in ilk durumunu bulmak en fazla $(2^{L_1}-1)$ deneme gerektirir. Eğer diğer LFSR'ların çıktıları ile anahtar dizisi arasında korelasyon varsa aynı yöntem kullanılarak ilk durmları elde edilebilir. Sonuç olarak $\sum_{i=1}^{n}(2^{L_i}-1)$ deneme gerekmektedir. Bu ise $\prod_{i=1}^{n}(2^{L_i}-1)$ göre daha küçük bir sayıdır. Aynı şekilde LFSR'ların belli bir kombinasyonu ile çıktı arasındaki korelasyonda analiz için kullanılabilir.

Örnek:

Geffe üreteci olarak bilinen aşağıdaki sisteme korelasyon atağı uygulayacağız.



Geffe üretici

$z = f(x_1, x_2, x_3) = x_1 \oplus x_2(x_1 \oplus x_3)$

x_1	x_2	x_3	$\Rightarrow$	z
0	0	0		0
0	0	1		0
0	1	0		0
0	1	1		1
1	0	0		1
1	0	1		1
1	1	0		0
1	1	1		1

$P(z = x_1) = \frac{6}{8} = 0.75, \;\; P(z = x_2) = \frac{4}{8} = 0.5, \;\; P(z = x_3) = \frac{6}{8} = 0.75$

Görüldüğü gibi f fonksiyonunun çıktıları 0.75 ihtimalle x_1 ve x_3 ile tutuyor. Dolayısıyla f fonksiyonu yeteri kadar çıktısı elde edilirse 3 LFSR'ın başlangıç konumlarını bulunabilir.

8.4 Blok Şifrelerin Analizi

Blok şifrelerin analizinde en kuvvetli analiz metodları olarak bilinen iki analiz yöntemini inceleyeceğiz. Biham ve Shamir tarafından geliştirilen difransiyel kriptanaliz (differential cryptanalysis) ve Matsui tarafından geliştirilen doğrusal kriptanaliz (linear cryptanalysis).

8.4.1 Difransiyel Kriptanaliz

Difransiyel Kriptanaliz methodu DES, GDES, Lucifer, FEAL, PES, IDEA, LOKI'89, REDOC ve Khafre dahil olmak üzere bir çok sayıda blok şifre sistemine uygulanmış bir seçilmiş açık metin atağıdır. Biham ve Shamir tarafından geliştirilen bu atak, ilk önce DES in indirgenmiş döngü çeşitlerine ve sonra tüm 16-döngü DES e uygulanmıştır.

Günümüzde bilinen en önemli ataklardan birisidir çünkü DES in anahtarları teorik olarak tüm anahtar uzayını denemeyle beklenen masraftan daha azı ile elde edilebilinmektedir. Difransiyel Kriptanaliz, kripto sistemlerin yeniden gözden geçirilmesine, tekrar dizyan edilmesi ve yeni sistemlerinin bu atağa karşı dayanıklı tasarlanmalarına neden olmuştur.

Bu kriptanaliz metodu açık metin ikilileri farkının bunlara karşılık gelen kapalı metin ikilileri üzerindeki etkisini kullanarak analiz yapıar. Bu farklar olası anahtarları ihtimal atamak ve ihtimali en yüksek anahtarları belirlemek için kullanılır. Aynı farka sahip olan bir çok açık metin ikilisini ve karşı gelen kapalı metin ikililerini kullanır.

2n-bit blok şifre sistemleri için Difransiyel Kriptanalizin özet tanımını vereceğiz. İlk olarak eşit uzunluktaki iki bit dizinin X ve $\acute{X}$ arasındaki **farkı** (difference) tanımlayalım:

$$\Delta X = X \otimes \acute{X}^{-1}$$

Burada $\otimes$ bit dizi grupları üzerinde, döngü (round) fonksiyonu içinde anahtar ile metin girdisinin birleştirilmesini sağlayan bir grup operasyonudur ve $\acute{X}^{-1}$ $\otimes$ operasyonuna göre X in tersidir. Yukarıdaki farkı tanımlamada asıl amaç metin girdileri arasındaki farkın anahtar eklenmeden ve eklendikten sonra aynı olması yani farkın anahtardan bağımsız yapılması çabasıdır. Bu bakış açısını anlamak için :

$$\Delta X = (X \otimes K) \otimes (\acute{X} \otimes K)^{-1} = X \otimes K \otimes K^{-1} \otimes \acute{X}^{-1} = X \otimes \acute{X}^{-1}$$

Feistel yapısındaki blok şifre sistemlerinin bir çoğu için bu farkı kullanarak şifre sistemin bir döngüsü için olası tüm metin girdi farklarına ve bunlara karşılık gelen olası çıktı farklarının ilgili olasılıklarını içeren fark dağılım tabloları oluşturmak mümkündür.

Açık metinimiz $P = C_0$ ve C_i de i döngü şifrelemesinden oluşan kapalı metin olsun. α_i ΔC_i nin beklenen değeri ve α_0 seçilen $\Delta P = \Delta C_0$ olmak üzere bir **r-döngü karakteristiği** $(r+1)$ lik $(\alpha_0, \ldots, \alpha_r)$ dır. Burada ΔP açık metin farkı ve ΔC_i de i inci döngüden sonraki kapalı metin farkıdır. Bir karakteristiğin olasılığı verilen $i-1$ döngü şifrelemesinden oluşan $\Delta C_{i-1} = \alpha_{i-1}$ farka göre i döngü şifrelemesinden sonra elde edilen $\Delta C_i = \alpha_i$ farkının edilmesinin koşullu olasılığıdır. Rastgele, hep aynı şekilde seçilmiş döngü anahtarları K_i ler için bir karakteristiğin olasılığı

$$\Pr(\Delta C_{i-1}{=}\alpha_i, \Delta C_{i-1}{=}\alpha_{i-1}, \ldots, \Delta C_1 = \alpha_1 \mid \Delta P = \alpha_0)$$

Bu olasılığı hesaplamak çok zor olabilir. Bununla beraber bazı blok şifre sistemleri için bu olasılık her bir döngünün olasılıkları kullanılarak hesaplanabilir (Markov şifre sistemleri). İstatistiksel işlemleri kolaylaştırmak adına bundan sonra döngü anahtarlarının bağımsız ve hep aynı şekilde rastgele seçildiklerini varsayacağız.

Açık metin ikilisi P ve $\acute{P}$ farkı ΔP, anahtar K ve r-döngü karakteristiğine göre **doğru ikili** olarak adlandırılabilinmesi için P ve $\acute{P}$ şifrelendikten sonra arada yer alan döngülerin kapalı metinlerinden oluşan farklar r-döngü karakteristiği izlemelidir. Eğer anahtar K ve r-döngü karakteristiğine göre P ve $\acute{P}$ doğru ikili değilse **yanlış ikili** olarak adlandırılırlar. p karakteristik olasılığı olmak üzere 2n-bitlik şifre sistemi için yaklaşık $p.2^{2n}$ doğru ikili bulunmaktadır.

Difransiyel Kriptanalizin amacı son döngüde kullanılan K_r anahtarını belirlemektir. Bazı açık metin ikilileri için C_r ve $\acute{C_r}$ kapalı metinler olsun. Seçilmiş açık metin atağında kriptanalist, blok şifre sistemin son döngüsü girdileri C_{r-1} ve $C_{r-1}^{'}$ bilemez fakat seçilen

karakteristiğe göre $r-1$ döngü şifre sonundaki kapalı metinlerin farkı ΔC_{r-1} tamamen veya kısmi olarak p olasılıkla bilir. Ve sonra verilen açık metin P ve $\acute{P}$ ikilisinin farkı ΔP için kriptanalist aşağıdaki denklemi K_r yi çözmeye çalışır:

$$g^{-1}(C_r, K_r) \otimes g^{-1}(\acute{C}_r, K_r)^{-1} = \Delta C_{r-1}$$

Yukarıdaki denklemin çözümü aday döngü anahtarları olarak adlandırabileceğimiz $k_1, k_2, \ldots, k_j$ olsun. Eğer P ve $\acute{P}$ doğru ikili ise $K_r \in \{k_1, k_2, \ldots, k_j\}$. Eğer P ve $\acute{P}$ yanlış ikili ise k_i nin K_r den bağımsız olduğunu kabul edilir. Sonrası eğer çok miktarda P ve $\acute{P}$ ikilileri denenirse, aday anahtarların tekrarı kaydedilir ve doğru döngü anahtarı K_r diğer adaylara göre daha fazla sayılmasını bekleriz. Difransiyel Kriptanaliz methodu aşağıdaki basamaklarla özetlenebilir:

- Tamamen veya kısmı olarak yüksek olasılıkta ΔC_{r-1} i veren bir $(\Delta P, \Delta C_1, \Delta C_2, \ldots, \Delta C_{r-1})$ r-döngü karakteristiği bulunması.
- Doğru ikili olduğunu varsaydığımız hep aynı şekilde P ve $\acute{P}$ açık metin ikilisi (farkları ΔP) yardımıyla aday döngü anahtarları $k_1, k_2, \ldots, k_j$, herbiri k_i gözlemlenen çıktı farkını verenler olmak üzere seçilir. Her aday döngü anahtarı k_i için sayaç bir arttırılır.
- Üsteki iki basamak bir aday anahtar k_i diğerlerine göre çok sayıda sayılana kadar tekrar edilir. En çok sayılan k_i gerçek r-döngü anahtarı K_r olarak kabul edilir.

Difransiyel Kriptanalizin karmaşıklığını tanımlamak için anahtar veya döngü anahtarını belirlemek için seçilen farka göre şifrelenen açık metin ikililerin sayısı kullanılabilir.

Sınırlandırılmış DES sürümleri üzerinde Biham ve Shamir (DES kitabi referans olacak) atağın karmaşıklığını yaklaşık olarak c/p bulmuşlardır (p kullanılan karakteristiğin olasılığı ve c sabit sayı ve $2 \prec c \prec 8$ olmak üzere).

Difransiyel Kriptanaliz seçilmiş açık metin atağı olmasına karşın kullanılan metin ikilileri arttırılarak bilinen metin atağında da çalışması sağlanabilir.

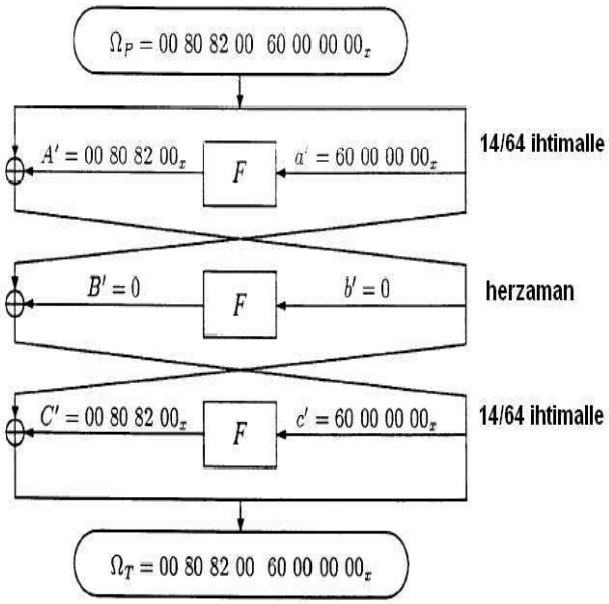
DES şifre sistemini ele aldığımızda yukarıda bahsedilen metodun uygulanması için farklar kullanılarak aşağıdaki gibi bir **XOR** tablosu oluşturulur.

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
2_x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3_x	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
4_x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
5_x	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
6_x	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
7_x	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
8_x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
9_x	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
A_x	0	8	6	2	2	8	6	0	6	4	8	0	4	0	2	10
B_x	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
C_x	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
D_x	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
E_x	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
F_x	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
									⋮							
30_x	0	4	6	0	12	6	2	2	8	2	4	4	6	2	2	4
31_x	4	8	2	10	2	2	2	2	6	0	0	2	2	4	10	8
32_x	4	2	6	4	4	2	2	4	6	6	4	8	2	2	8	0
33_x	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4
34_x	0	8	16	6	2	0	0	12	6	0	0	0	0	0	8	0	6
35_x	2	2	4	0	8	0	0	0	14	4	6	8	0	2	14	0
36_x	2	6	2	2	8	0	2	2	4	2	6	8	0	4	10	0
37_x	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4
38_x	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10
39_x	6	2	2	4	12	6	4	8	4	0	2	4	2	4	4	0
$3A_x$	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	0
$3B_x$	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2
$3C_x$	0	10	4	0	12	0	4	2	6	0	4	12	4	4	2	0
$3D_x$	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4
$3E_x$	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
$3F_x$	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

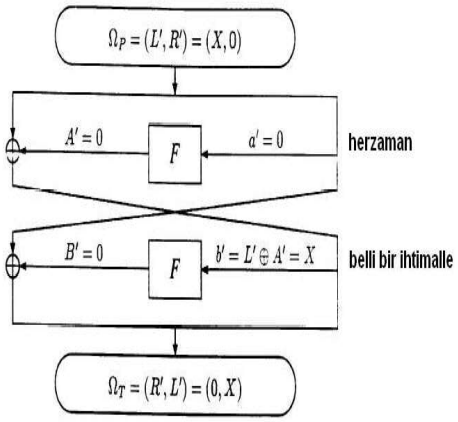
XOR-tablosu (1. S-kutusunun)

DES'in çeşitleri döngü sayılarına göre atağın başarı durumları aşağıdaki tabloda verilmiştir.

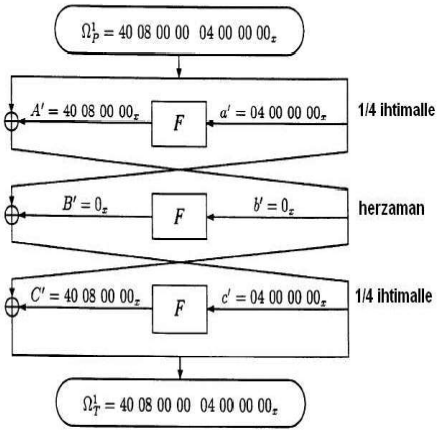
Rounds	Complexity
4	2^4
6	2^8
8	2^{16}
9	2^{26}
10	2^{35}
11	2^{36}
12	2^{43}
13	2^{44}
14	2^{51}
15	2^{52}
16	2^{58}



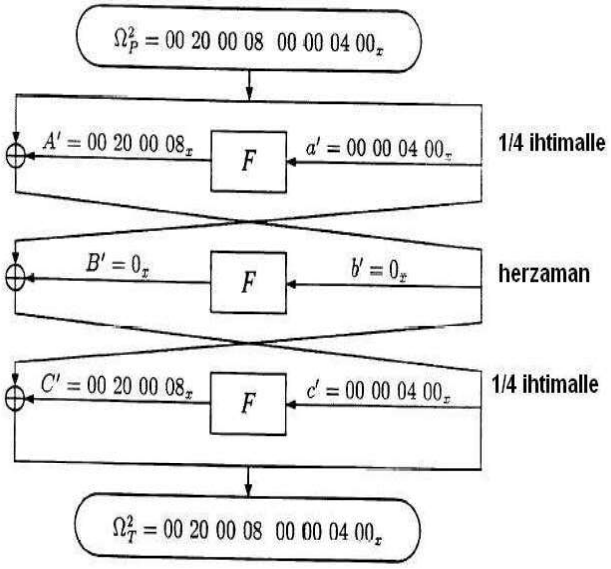
3-round (step) Karakteristik



(iterative) karakteristik tekrar edilebilen



3-round karakteristik



3-round karakteristik

8.4.2 Doğrusal Kriptanaliz

Doğrusal Kriptanaliz 1993 yılında DES sistemini kırmak için Matsui tarafından geliştirilmiş bir bilinen açık metin atak çeşididir. 2^{47} açık metin kullanılarak DES sistemi kırılmıştır. Doğrusal olmayan (nonlinear) fonksiyonlara doğrusal (linear) fonksiyonlarla yaklaşarak yapılmıştır. Bu yaklaşım olasılık üzerine dayalı olduğu için 0.5'ten ne kadar sapılırsa fonksiyonun yerine doğrusal fonksiyonlar kullanmak bu sapma miktarı kadar avantaj kazandırır.

$$P[i_1, i_2, ..., i_a] \oplus C[j_1, j_2, ..., j_b] = K[k_1, k_2, ..., k_c] \ ,$$

$i_1, i_2, ..., i_a, j_1, j_2, ..., j_a$ ve $k_1, k_2, ..., k_c$ belirli bit yerlerini göstermektedir, ve yukarıdaki denklemin tutma ihtimali $p \neq \frac{1}{2}$.

Yukarıdaki efektif doğrusal ifadeye ulaşıldıktan sonra anahtar bitleri aşağıdaki maksimum yakınlık metodu ile bulunur.

Algoritma

Adım 1 : Yukarıdaki denklemin sol tarafının 0'a eşit olduğu açık metinlerin sayısı T olsun.

Adım 2 : Eğer $T > N/2$ (Denenen açık metin sayısı = N),

$\longrightarrow K[k_1, k_2, ..., k_c] = 0$ (eğer $p > \frac{1}{2}$) veya 1 (eğer $p < \frac{1}{2}$)

$\longrightarrow K[k_1, k_2, ..., k_c] = 1$ (eğer $p > \frac{1}{2}$) veya 0 (eğer $p < \frac{1}{2}$)

Aşağıdaki tabloda N ve p cinsinden atağın başarı oranları verilmiştir.

N	$\frac{1}{4}\|p-\frac{1}{2}\|^{-2}$	$\frac{1}{2}\|p-\frac{1}{2}\|^{-2}$	$\|p-\frac{1}{2}\|^{-2}$	$2\|p-\frac{1}{2}\|^{-2}$
Başarı oranı	84.1%	92.1%	97.7%	99.8%

Doğrusal kriptanaliz aşağıda kısaca özetlenmiştir.

- Efektif doğrusal ifadenin bulunması,
- Başarı oranının N ve p cinsinden ifadesi,
- En iyi doğrusal ifadenin ve anahtar için en iyi tutma ihtimalinin hesaplanması.

Kaynaklar:

[1] J.Daeman,R. Govaerts and J. Vandewalle, *Weak Keys for IDEA*, Advances in Cryptology, Proc. EUROCRYPTO'93, LNCS 773, Springer-Verlag, pp. 224-231, 1994.

[2] A. Biryukov, *Introduction to cryptology and cryptanalysis* (Ders Notu), http://www.wisdom.weizmann.ac.il/ albi/cryptanalysis/lectures.htm

[3] X. Lai, J. L. Massey and S. Murphy, *Markov Cipher and Differential Cryptanalysis*, Advances in Cryptology, EUROCRYPTO'91, Lecture Notes in Computer Science, Springer Verlag, Berlin-Heidelberg, 547, pp. 17-38, 1991

[4] X. Lai, *On the design and security of block cipher*, ETH Series in Information Processing, V.1, Konstanz: Hartung-Gorre Verlag, 1992.

[5] *NESSIE Project: New European Schemes for Signatures, Integrity and Encryption at*, http://cryptonessie.org

[6] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, http://www.cacr.math.uwaterloo.ca/hac/

[7] L. R. Knudsen, *Ph.D. thesis: Block ciphers - Analysis, Design and Applications* , http://www.mat.dtu.dk/people/Lars.R.Knudsen/thesis.html

[8] *Crypto papers*, http://www.funet.fi/ bande/docs/crypt/