BÖLÜM 1

GİRİŞ

Şifre sistemleri *açık anahtarlı* ve *gizli anahtarlı (simetrik)* olmak üzere ikiye ayrılır. Açık anahtarlı sistemlerde her kişi, biri açık diğeri gizli olmak üzere bir çift anahtar edinir. Açık anahtar diğer kullanıcıların erişimine açıkken; gizli anahtar sadece sahibinin erişebileceği şekilde saklanmalıdır. Açık anahtarı kullanarak herhangi bir kişi şifreli mesaj gönderebilir, ancak gönderilen şifreli mesajı sadece kullanılan açık anahtarın eşi olan gizli anahtar açabilir. Açık anahtarlı şifre sistemleri sadece şifreli mesaj göndermek amacıyla değil, kimlik denetimi yani sayısal imza ve daha birçok teknik için kullanılır. Açık anahtarlı sistemlerde, her zaman gizli anahtarın açık anahtarla matematiksel bir bağıntısı vardır. Bu anahtarları oluşturmak için çözülememiş matematik problemleri kullanıldığından, açık anahtarı kullananarak gizli anahtarı elde etme işlemi de imkansız kabul edilir.

Örnek 1.0.1 A, B kullanıcılar, K_A, K_B kullanıcıların açık anahtarları ve K'_A, K'_B kullanıcıların gizli anahtarları olsun. Her bir kullanıcı diğerlerinin açık anahtarını bilir. B kullanıcısı A kullanıcısına bir mesajı göndermek için mesajı K_A ile şifreleyip gönderir, A kullanıcısı şifrelenmiş mesajı K'_A ile deşifre eder.

Açık anahtarlı sistemleri ayrıntılı olarak ilerki konularda öğreneceğiz. Öncelikle gizli anahtarlı yani simetrik sistemlerden bahsedelim. Simetrik sistemlerde tek bir anahtar, hem şifreleme hem de deşifre amacıyla kullanılır. Güvenli bir şekilde iletişim kur-

madan önce gönderici ile alıcının gizli anahtar olarak adlandırılan bir anahtar üzerinde uzlaşmaları gerekir.

Simetrik sistemlerde temel problem, göndericinin ve alıcının üçüncü bir kişinin eline geçmesini engelleyerek ortak bir anahtar üzerinde anlaşmalarıdır. Ancak simetrik sistemlerin avantajı da, açık anahtarlı sistemlere göre daha hızlı olmalarıdır.

Bir sistemin güvenliği anahtarda yatar. Şifre çözmeye yönelik ataklar anahtarı bulmaya yöneliktir. Kriptanalist sahip olduğu ön bilgiye göre farklı saldırı çeşitleri uygular. Bunlar:

Sadece Şifreli Metin Saldırısı : Kriptanalist, aynı şifreleme algoritması kullanılarak şifrelenmiş çeşitli açık metinlerin şifreli metinlerine sahiptir. Kriptanalist mümkün olduğunca çok sayıdaki şifreli metinin açık metnini bulmaya çalışır. Asıl önemli olan ise açık metinleri şifrelemek için kullanılan anahtarı ya da anahtarları, aynı anahtarla şifrelenen başka mesajları çözmek için bulmaktır.

Bilinen Açık Metin Saldırısı : Kriptanalist sadece çeşitli açık metinlerin şifrelenmiş haline değil, bu mesajların açık metinlerine de erişebilmektedir.

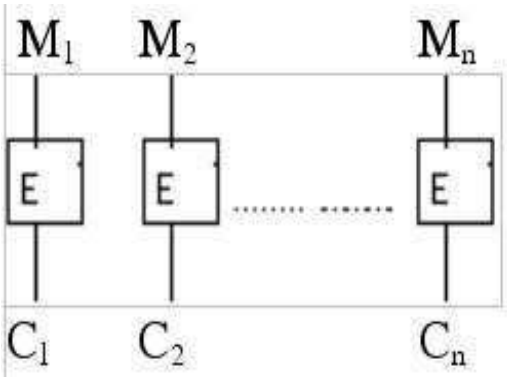
Seçilmiş Açık Metin Saldırısı : Kriptanalist sadece çeşitli açık metinlerin şifreli metinlerine ve bunlarla ilişkilendirilmiş açık metinlere erişmekle kalmayıp, aynı zamanda da şifrelenmiş açık metinleri seçebilmektedir. Bu atak bilinen açık metin atağından daha güçlü bir ataktır. Çünkü kriptanalist şifrelemek için açık metinin belirli bloklarını yani anahtar hakkında daha fazla bilgi sağlayabilecek olanları seçebilmektedir.

Simetrik sistemler *Blok Şifre Sistemleri* ve *Akan Şifre Sistemleri* olarak ikiye ayrılır.

BÖLÜM 2

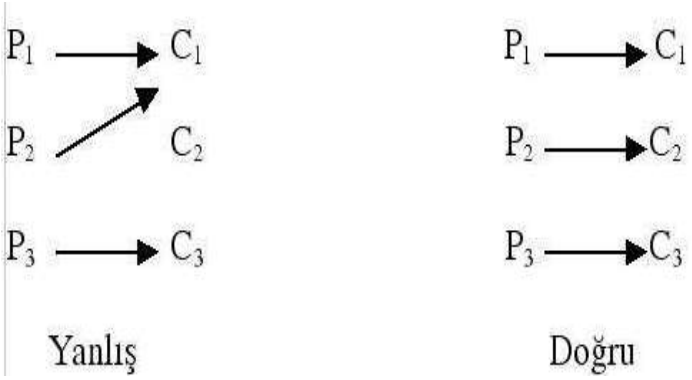
BLOK ŞİFRELER

Blok şifrelemenin en basit tanımı, açık metni bitişik bloklara bölme, her bloğu şifreleyerek şifreli metin bloklarına dönüştürme, bu şifreli blokları şifreli metin çıkışı olarak gruplamaktır. Blok şifre sistemini şekille göstermek istersek, M_1, $M_2, \ldots, M_n$ açık metnin blokları, yani her biri k bitten oluşan ardışık parçaları, C_1, $C_2, \ldots, C_n$ bu bloklara karşılık gelen şifrelenmiş metinler ve E şifreleme işlemi olmak üzere, blok şifre sistemlerini aşağıdaki şemayla gösterebiliriz.



Blok şifre Sistemlerinde şifreleme

Çoğu blok şifre sistemlerinde blok uzunluğu 64 bittir. İşlemcilerin hızı arttıkça blok uzunluğu da artabilmektedir. Son yıllarda üretilen sistemler 128 bit blok uzunluğu kullanılmaya başlanmıştır.



Bir blok şifre sisteminde, şifreli metin bloklarından birinin kaybolması, diğer blokların deşifre işleminde bir yanlışlığa neden olmaz. Bu blok şifre sistemlerinin en büyük avantajıdır. Blok şifre sistemlerinin en büyük dezavantajı ise şifreli metindeki birbirinin aynısı olan blokların, açık metinde de birbirinin aynı olmasıdır.

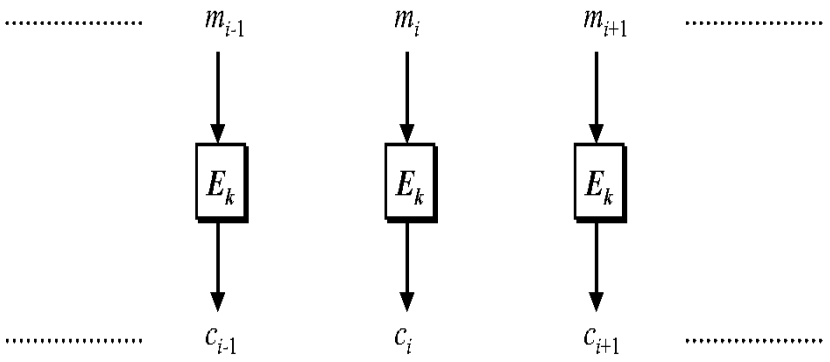
Örnek 2.0.2 "Senay'a kitabı sen ver" cümlesini, blok uzunluğu 3 olacak şekilde bölüp şifrelersek,

Açık Metin: sen-aya-kit-abı-sen-ver
Şifreli Metin: axk-bcg-xkt-ase-axk-hyt

birinci ve beşinci blokların aynı şekilde şifrelendiğini görüyoruz.

Böyle bir sorunun üstesinden gelmek için şifreleme işlemini değişik modellerle yapabiliriz. M_{i-1}, M_i, M_{i+1} açık metnin ardışık 3 bloğu, E şifreleme işlemi, C_{i-1}, C_i, C_{i+1} M_{i-1}, M_i, M_{i+1} ardışık bloklarının şifreli halleri olsun.

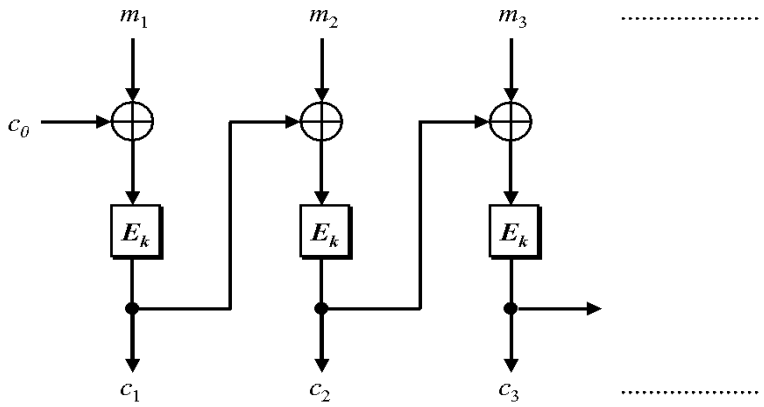
1. *Elektronik Kod Modeli* (Electronic Code Mode)



Elektronik Kod Modeli

Örnekteki gibi işler.

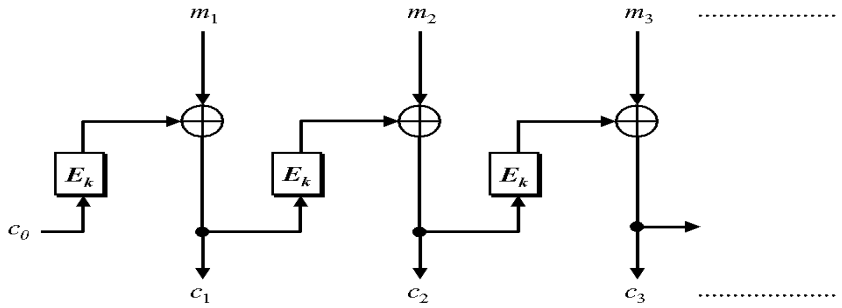
2. *Kapalı Metin Zincirleme Modeli* (Cipher Block Chaining Mode)



Kapalı Metin Zincirleme Modeli

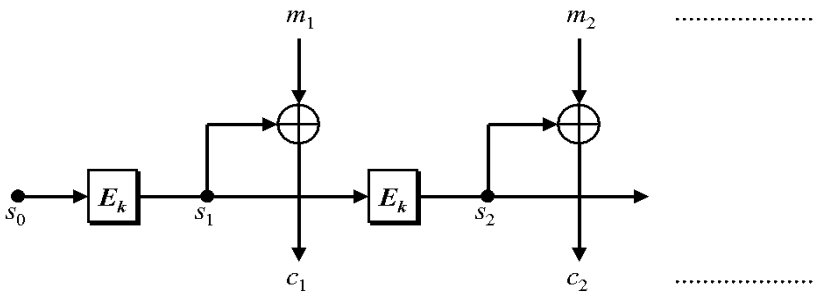
Aslında bu modelde yaptığımız işlemleri, büyük bloklar üzerinde akan şifre sistemini uygulamak olarak görebiliriz.

3. *Çıktıyı Geribesleme Modeli* (Output Feedback Mode)



Çıktıyı Geribesleme Modeli

4. *Girdiyi Geribesleme Modeli* (Input Feedback Mode)



Girdiyi Geribesleme Modeli

Bir blok şifre sisteminin matematiksel olarak şöyle tanımlayabiliriz. $\mathbb{Z}_2 = \{0\,1\}$, $\mathbb{Z}_2^n = \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2 = \{(x_{n-1}, \ldots, x_0) : \ x_i \in \mathbb{Z}_2\}$ ve K ise anahtar uzayı olsun. $E : \mathbb{Z}_2^n \times K \to \mathbb{Z}_2^n$

ve her $k \in K$ için $E(p,k)$ tersi alınabilir bir fonksiyondur. Bu fonksiyona şifreleme fonksiyonu denir. Blok şifre sistemi ile şifrelenen bir mesajı deşifre ederken aynı sistemi şifreli mesaja aynı anahtar ile uygulamak gerekir. Bunun için şifreleme işleminin tersinin olması gerekir. Şifreleme fonksiyonunun tersine de deşifreleme fonksiyonu denir ve $D(c,k)$ ile gösterilir.

2.1 Blok Şifre Sistemlerinin Parametreleri

2.1.1 Blok Uzunluğu

Bir blok şifre sisteminin güvenli olabilmesi için, blok uzunluğunun bazı blokların diğerlerinden daha fazla görünmeyeceği şekilde uzun olması gerekir. Örneğin bir blok şifreleme sistemi olan DES'teki 64 bit uzunluk, sıklık analizine karşı DES'i güçlü kılmaktadır. Aynı zamanda blok uzunluğu n olan bir blok için, sabit bir anahtarla saldırı yapan kişinin elde edebileceği açık metin-şifreli metin çiftlerinin sayısı büyük olmalıdır (bu sayı 2^n yi geçemez). Blok uzunluğu büyüdükçe sistemin uygulaması da daha karışık hale gelmektedir.

2.1.2 Anahtar ve Gerçek Anahtar Uzunluğu

Bir blok şifre sisteminin anahtarı deneme-yanılma (exhaustive key search) ile bulunamamalıdır. Bunun için de anahtar uzun olmalıdır. Diğer taraftan da anahtar uzunluğu üretim, dağıtım ve saklama için uygun ve güvenilir olmalıdır. Örneğin DES her zaman anahtar uzunluğunun kısa olmasından dolayı eleştirilmiştir. Diffie ve Hellman

DES'in anahtar deneme-yanılma yolu ile 20 milyon dolara mal olacak bir sistemle 12 saatte kırılabileceğini öne sürdüler. Gelen öneriler doğrultusunda, DES'in gerçek anahtar uzunluğu 128 bite çıkarıldı ve üçlü şifreleme ile DES daha güvenli bir şekilde kullanılabilir hale getirildi.

2.2 Blok Şifre Sistemlerinin Tasarım Ölçütleri

Güvenli bir blok şifre sisteminin kırılması zor ama uygulaması kolay olmalıdır. Şifreleme ve deşifreleme fonksiyonlarının kolay uygulanabilir olması gerekirken, $C = E(P, k)$ ve $P = D(C, k)$ eşitliklerinden k yı bulmanın zor olması gerekir. ilk defa Claude Shannon tarafından önerilen tasarım ölçütleri *yayılma* (confusion) ve *nüfuz etme* (diffusion)dir.

2.2.1 Yayılma

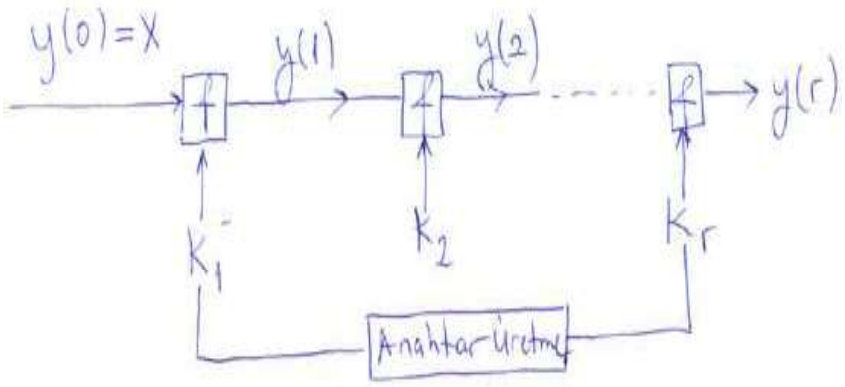
Bir blok şifre sistemini ya da genel olarak bir şifreleme sistemini yayılma ölçütüne göre tasarlamak demek, şifreli metinle anahtar arasındaki ilişkiyi mümkün olduğunca karışık yapmaktır. Daha açık bir tanım verirsek, yayılma, anahtarın açık ve şifreli metne bağlılığının kriptanaliz için faydalı olmayacak kadar karışık olması demektir. Yani blok şifre sistemini tanımlayan eşitliklerin doğrusal olmaması ve karışık olması ve böylece $C = E(P, k)$ denkleminden anahtarı bulmanın imkansız olması gerekir.

2.2.2 Nüfuz Etme

Bu ölçüte göre her anahtar için şifreleme fonksiyonu öyle olmalı ki, açık metin ve şifreli metin arasındaki yapılar arasında istatiksel bağlılık olmamalıdır. Bu ölçütün olabilmesi için anahtarın ve açık metinin her bitinin şifreli metini etkilemesi gerekir.

2.3 Döngülü (Iterated) Blok Şifre Sistemleri

Aynı fonksiyonu belli döngüler içinde uygulayan sistemlere döngülü blok şifre sistemleri denir.



Döngülü (Iterated) Blok Şifre Sistemleri

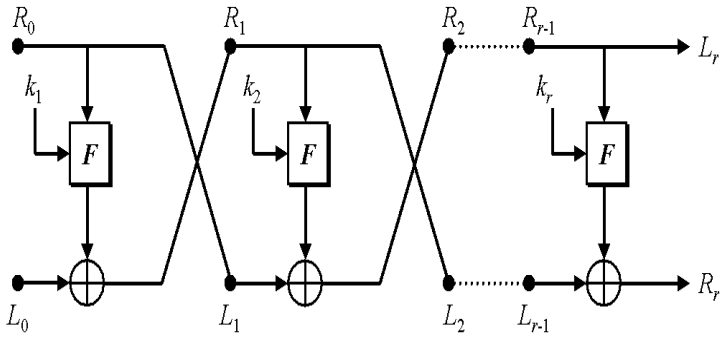
Fonksiyonun ilk kullanım hariç girdisi; bir önceki döngünün çıktısıdı ve anahtar üreten algoritmadan elde edilen döngü anahtarıdır. Örneğin DES'te 16 döngü vardır. Algoritmada

kullanılan f fonsiyonu basit bir fonksiyon olursa uygulamada bize hız yönünden kolaylık sağlar. Döngü sayısı uygun şekilde seçilirse, sistemde gereken yayılma ve nüfuz etme sa?lanır. Bu tür sistemlerde döngü sayısı, sistem tasarlandıktan sonra belli saldırılara karşı dayanıklılığı hesaplanarak belirlenmektedir.

2.4 Feistel Yapılar

Horst Feistel tarafından ilk defa tasarlanan sistem günümüzde birçok modern sistemde kullanılmaktadır.

$k_1, k_2, \ldots, k_n$: Döngü Anahtarları olmak koşuluyla , Feistel yapılarını aşağıdaki gibi gösterebiliriz.



Feistel Yapısı

Şifreleme yapılırken L bloğu üzerine, deşifreleme yapılırken R bloğu üzerine işlem yapılmaktadır. Ancak deşifreleme işleminde döngü anahtarları, ters sırada kullanılmaktadır.