



Simetrik Şifreleme ve Mesaj Gizliliği

Dr. Fatih KALEMKUŞ

Kafkas Üniversitesi

- Bilginin güvenli bir şekilde iletilmesi ihtiyacı çok **eski zamanlara** dayanır.
- İlk gizli bilgi paylaşımı yöntemleri, savaş ortamında hükümdarın verdiği emirlerin, düşman kuvvetlerinin eline geçmeden askerlerini yönetmek amacıyla kullanılması için ortaya çıkmıştır
- Zaman içinde **bilişim teknolojilerinin gelişmesiyle**, haberleşme, savunma, bankacılık gibi birçok alanda bilginin gizli olarak, değişime uğramadan iletilmesi ve sadece yetkili kişiler tarafından okunması ihtiyacı artan bir öneme sahip olmuştur.

Kriptoloji

Kriptoloji, kriptografi ve kriptoanaliz olmak üzere ikiye ayrılır.

- **Kriptografi**, güvenli veri paylaşımı için gerekli algoritmaları ve protokolleri ortaya koyar.
- **Kriptoanaliz**, kriptografik algoritmaların, varsa açıklarını tespit ederek, onları kırmaya çalışır.

Kriptografi, kullanıcılar arasında güvenli bir iletişim oluşturmak için gerekli algoritmaları ve protokolleri tasarlayan ve geliştiren bilim dalıdır.

Kriptoanaliz

Kriptoanaliz ile ilgilenen ve üzerinde arařtırmalar yapan **iki grup** vardır.

- **Birinci grup**, algoritmalaradaki açıkları ve eksiklikleri tespit ederek, kendilerine çıkar sağlamaya çalışan kişilerden oluşur.
- **İkinci grup**, genellikle bilim adamlarından oluşur ve algoritmaların varsa açıklarını tespit ederek, kimse zarar görmeden bu açıkların giderilmesini sağlarlar.

Simetrik Şifreleme Algoritmaları

Bilginin güvenilir bir şekilde saklanması ve iletilmesi için kriptografik algoritmalar ve protokoller tercih edilir.

Kriptografik algoritmalar ve protokoller dört temel alanda gruplandırılır. Bu gruplar;

1. Simetrik şifreleme
2. Açık anahtar şifreleme
3. Veri bütünlüğü
4. Kimlik doğrulama

Şifreleme algoritmaları;

1. Tek anahtar kullanan şifreleme algoritmaları (simetrik şifreleme algoritmaları)
2. Birbiriyle ilişkili iki anahtar kullanan şifreleme algoritmaları (açık anahtar şifreleme algoritmaları)
3. Anahtar kullanmayan algoritmalar (özetleme fonksiyonları)

Şifreleme Algoritmaları

- **Simetrik şifrelemede** tek anahtar kullanıldığından, bu şifreleme algoritmaları “**tek anahtar şifreleme**” ve “**gizli anahtar şifreleme**” algoritmaları olarak da bilinirler.
- **Simetrik şifreleme** algoritmalarına simetrik denmesinin nedeni, **şifreleme ve çözme için tek ve aynı anahtar** kullanılmasıdır.
- **Açık anahtar** şifreleme algoritmalarında ise **açık ve gizli olmak üzere iki anahtar** kullanılır.
- Bunlardan biri şifreleme diğeri ise çözme işlemleri için kullanılır. Bu nedenle iki anahtarlı bu algoritmalar, asimetrik şifreleme algoritmaları olarak da adlandırılır.
- **Özetleme** algoritmaları ise **veri bütünlüğünün kontrolü** amacıyla kullanılmaktadır.

Şifreleme Algoritmaları

Simetrik Şifreleme

- Simetrik algoritmalarda, mesajın gizliliğini sağlayarak haberleşmek isteyen **gönderici** ve **alıcı** aynı algoritmayı kullanır.
- Simetrik şifrelemede kullanılan tekil anahtar gizli tutulmalıdır.
- Bu anahtarı sadece gönderici ve alıcının bildiği varsayılır.

Açık Anahtar Şifreleme

- Açık anahtar şifrelemede **kullanılan algoritma aynı** olmasına rağmen şifreleme ve şifre çözmek için farklı anahtarlar kullanılır.
- Bu anahtarlar matematiksel olarak birbiriyle ilişkili anahtarlardır.
- Açık anahtar şifrelemede **gizli anahtarın** sadece anahtar sahibi tarafından bilinmesi gerekirken, **açık anahtarın** diğer kullanıcılar tarafından bilinmesinde hiçbir mahsur yoktur.

Simetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmalarının **beş temel ögesi** vardır. Bunlar;

- Açık metin
- Şifreleme fonksiyonu
- Gizli anahtar
- Şifrelenmiş metin
- Çözme fonksiyonu

Simetrik Şifreleme Algoritmaları

Açık Metin

- Kullanıcının oluşturduğu ve güvenli şekilde paylaşmak istediği orijinal veridir.
- Şifreleme algoritmasının girdilerinden bir tanesidir.
- Açık metin, gizlenmek istenen her türlü metni ifade etmektedir.
- Açık metin, bir e-posta mesajı olabileceği gibi, bir resim dosyası, bir kitap bölümü veya bir sayı dizisi de olabilir.

Simetrik Şifreleme Algoritmaları

Şifreleme Fonksiyonu

- Açık metin yetkisi olmayan kişiler tarafından okunmaması için karıştırma işlemi yapmaktan sorumludur.
- Simetrik algoritmalarda , şifreleme sırasında kullanılan iki ana fonksiyon karışıklık ve yayılma fonksiyonlarıdır.
- Şifreleme fonksiyonu çok sayıda birbirini takip eden karışıklık ve yayılma işlemlerinden meydana gelir.

Simetrik Şifreleme Algoritmaları

Gizli Anahtar

- Simetrik şifreleme algoritmalarının **girdilerinden ikincisidir**.
- Bu anahtarı yalnızca güvenli iletişim kurmak isteyen kullanıcıların bildiği kabul edilir.
- Simetrik şifreleme algoritmalarının güvenliği bu anahtarın gizliliğine dayandığından, **gizli anahtarı yalnızca haberleşmekte olan iki kullanıcının bilmesi** gerekmektedir.
- Bu anahtarın başkaları tarafından ele geçirilmesi, iletişimin gizliliğini ortadan kaldıracaktır.

Simetrik Şifreleme Algoritmaları

Şifrelenmiş Metin

- Şifreleme algoritmasının çıktısıdır.
- Şifrelenmiş metni elde eden kötü niyetli kişiler, kullanılan algoritmayı bilseler dahi açık metin hakkında bir çıkarımda bulunamazlar.
- Şifreleme algoritmalarının bütün adımları herkes tarafından bilinmektedir.
- Güvenliği sağlayan, gizli anahtarın haberleşen kullanıcılar dışında kimse tarafından bilinmemesi ve gizli tutulmasıdır.

Simetrik Şifreleme Algoritmaları

Çözme Fonsiyonu

- Çözme fonksiyonunun girdileri şifrelenmiş metin ve gizli anahtardır.
- Çıktı olarak ise açık metin elde edilir.
- Simetrik şifrelemede, şifreleme ve çözme işlemleri birbirinin tersidir.
- Bu nedenle açık (düz) metni şifrelemek için gerçekleştirilen tüm işlemlerin ters fonksiyonları, şifreli metni çözmek için sondan başa doğru uygulanır.

Simetrik Şifreleme Algoritmaları

Bu temel bileşenler **değişkenlerle** ifade edilir;

- Açık veya düz metin (P)
- Şifrelenmiş metin (C)
- Gizli anahtar (K)
- Şifreleme fonksiyonu (E)
- Çözme fonksiyonu (D)

Önemli!!; simetrik şifreleme algoritmaları, **orijinal açık metnin şifreleme yöntemine** göre iki ana gruba ayrılabilir. Bu ölçüte göre simetrik algoritmalar, **blok** ve **dizi şifreleme algoritmaları** olarak sınıflandırılır.

- **Blok şifreleme**, şifrelenecek metin bloklar şeklinde şifrelenir ve çözülür. Blok şifreleme algoritmaları, belirli uzunluktaki (blok) açık metni girdi olarak alır ve yine belirli uzunlukta şifrelenmiş metin çıktısı üretirler.
- **Dizi şifreleme** algoritmaları ise açık metinden bir bit alıp gizli anahtarı kullanarak bir bit şifrelenmiş metin üretirler.

DİZİ ŞİFRELEME



Dizi şifreleme bit tabanlı bir simetrik şifreleme yöntemidir.

- Bağımsız olarak, açık metinden sıradaki tek biti kayar anahtar yardımı ile işleme tabi tutar ve karşılığında bir bitlik şifrelenmiş metin üretir.
- Dizi şifreleme yöntemleri, eşzamanlı ve eşzamansız olmak üzere ikiye ayrılır.
- Eşzamanlı dizi şifrelemesinde kayan anahtar üretimi sadece kullanıcının gizli anahtarına bağlıdır.
- Eşzamansız dizi şifrelemede ise kayan anahtar üretimi hem kullanıcının gizli anahtarına hem de bir önceki adımda üretilmiş şifrelenmiş metine bağlıdır.
- Dizi şifreleme bir örnekle şöyle açıklanabilir.
- Şifrelenmek istenen açık metin “merhaba” olsun.
- Dizi şifrelemede önce açık metnin ilk karakteri olan “m” şifrelenir.
- Daha sonra ikinci karakter olan “e” şifrelenir.
- Bu şekilde açık metnin bütün karakterleri sıra ile teker teker şifrelenmiş metne dönüştürülür.
- Şifreli metin alıcı tarafından aynı sırayla çözümlenerek açık metinde yer alan harfler elde edilir.

Dr. Fatik KALEMKUŞ

Rastgele Sayılar

- Rastgele sayılar kriptolojide büyük bir öneme sahiptir.
- Kriptolojik algoritmalarda kullanılacak rastgele sayıların iki önemli özelliği olmalıdır.
- Bu özellikler “rastgelelik” ve “tahmin edilemezlik” olarak adlandırılır.
- İstatistiksel olarak bir sayının rastgele olması için tekdüze dağılım göstermek ve bağımsız olmak üzere iki önemli özelliğe sahip olması gerekmektedir.
- Bilgisayar bilimlerinde üç farklı rastgele sayı vardır.
 1. Gerçek rastgele sayılar
 2. Sözde rastgele sayılar
 3. Kriptolojik olarak güvenli rastgele sayılar

Gerçek Rastgele Sayılar

- Para atışı işlemi sonucu gerçek rastgele sayı üretmek mümkündür.
- Para atışının 1.000 defa tekrar edilmesi durumunda büyük olasılıkla 500 defa tura ve 500 defa yazı gelmesi beklenir.
- İstatistiksel olarak bu sonuç, beklenen durumudur.
- Ama gerçekte sonuç bu şekilde çıkmayabilir.
- Yapılacak her para atışının tura mı yoksa yazı mı geleceği hiçbir şekilde bir önceki atıştaki sonuca bağlı değildir.
- Bir başka ifadeyle, para atışları birbirinden bağımsızdır.
- Para atışı işlemi, hem tekdüze dağılıma sahip olması hem de gelecek atışların önceki atışlara bağlı olmaması dolayısıyla rastgele sayılarda bulunması gereken iki özelliğe de sahiptir.
- Ancak tekrar üretebilme özelliği yoktur.
- Yani 100 atış sonunda elde edilen sonucu tekrar elde etmek çok düşük bir olasılıkla mümkündür ve garanti edilemez.

Gerçek Rastgele Sayılar

- Gerçek rastgele sayılar bu özellikleriyle oturum anahtarı üretilmesinde kullanılmaktadır.
- Oturum anahtarı, her orijinal açık mesajın şifrelenmesi için birbirinden bağımsız olarak üretilen anahtar demektir.
- Aynı gizli anahtar bütün mesajları şifrelemek için kullanılırsa güvenlik problemi oluşabilir.
- Çünkü bu anahtar bir şekilde elde edilirse, bu anahtarla şifrelenen mesajlara ulaşılmış olur.
- Ancak oturum anahtarı kullanılırsa her mesaj için bir anahtar kullanılmış olur.
- Bu durumda, anahtarlardan biri ele geçirilmiş olsa bile sadece bir mesaja ulaşılmış olur.
- Diğer mesajlara hala ulaşılamaz ve güvenlik sağlanmış olur.
- Oturum anahtarları belli şartlara göre rastgele üretilir.
- Bu nedenle gerçek rastgele sayılarla bu anahtarları üretmek önemlidir.

Sözde Rastgele Sayılar

- Birçok programlama dilinde var olan rastgele sayı üretici fonksiyonların (Örneğin; Java programlama dilinde `Math.random()`) ürettiği rastgele sayılar bu grupta yer alır.
- Bu fonksiyonlar belirli bir matematiksel fonksiyona bağlı olarak rastgele sayı üretirler.
- Dolayısıyla belirli sayıda üretilen rastgele sayı kullanılarak, ilgili matematiksel fonksiyona ait katsayılar hesaplanabilir.
- Sözde rastgele sayı fonksiyonları tekdüze dağılıma sahip olacak şekilde tasarlanmışlardır.
- Üretilen bir sayı dizisini, başlangıç parametreleri ve fonksiyon katsayılarının bilinmesi halinde tekrar üretmek mümkündür.
- Buna karşın, bir sonra üretilecek sayının tahmin edilmesi mümkün olduğu için kriptoloji algoritmalarında kullanım alanı sınırlıdır.

Kriptolojik Olarak Güvenli Rastgele Sayılar

- Tekdüze dağılıma sahiptir.
- Bir sonraki adımda üretilecek sayının tahmin edilemez.
- Başlangıç parametrelerinin bilinmesi durumunda aynı sayı dizisinin tekrar üretilebildiği rastgele sayılar bu grupta yer alır.
- Kriptolojik olarak güvenli rastgele sayılar dizi şifreleme algoritmalarında büyük bir öneme sahiptir.

Tek Zamanlı Blok

- Simetrik şifrelemede bir kullanımlık oturum anahtarları kullanmak önemlidir
- Kullanılacak gizli anahtarın, şifrelenecek açık veya düz metnin uzunluğu kadar olması ve sadece bir kez kullanılması durumunda, şifrelenmiş metni ele geçiren saldırgan, hiçbir matematiksel yöntem ile ne orijinal açık metni ne de gizli anahtarı elde edebilir.
- Bu tür yöntemlere, teorik olarak kırılmaz sistemler adı verilir.

Şifreleme fonksiyonu:

$$y_i = x_i + k_i \text{ mod } 2$$

Çözme fonksiyonu:

$$x_i = y_i + k_i \text{ mod } 2$$

DİZİ ŞİFRELEME

Tek Zamanlı Blok

Tek zamanlı blok veya bir kullanımlık oturum anahtarı ile şifrelemenin ve şifre çözmenin nasıl gerçekleştirildiğini sırasıyla Tablo 3.1 ve Tablo 3.2'deki gibi basit bir örnekle açıklayabiliriz.

Açık Metin	0	0	1	1	1	0	0	0
Anahtar Dizisi	1	1	1	0	0	1	1	0
Şifrenmiş Metin	1	1	0	1	1	1	1	0

Tablo 3.1
Tek zamanlı blok ile şifreleme örneği

Şifrenmiş Metin	1	1	0	1	1	1	1	0
Anahtar Dizisi	1	1	1	0	0	1	1	0
Açık Metin	0	0	1	1	1	0	0	0

Tablo 3.2
Tek zamanlı blok ile çözme örneği

x_i	k_i	y_i
0	0	0
0	1	1
1	0	1
1	1	0

Tablo 3.3
XOR doğruluk tablosu

DİZİ ŞİFRELEME

RC4

- Tek zamanlı blok yönteminin uygulamasında karşılaşılan zorlukları ortadan kaldırmak için sonsuz kayan anahtar yerine, belirli uzunlukta anahtar kullanan birçok çözüm ortaya konulmuştur.
- GSM şifrelemede kullanılan A5/1,A5/2 ve Wi-Fi güvenliğinde kullanılan RC4 gibi dizi şifreleme algoritmaları bu tür şifrelemelere örnektir.
- RC4, **Ron Rivest** tarafından **1987** yılında geliştirilmiştir
- 40 ila 256 bit arasında değişken boyutta gizli anahtar kullanmaktadır.
- Algoritmanın temeli rastgele karıştırmaya dayanmaktadır.

SSL (Secure Session Layer, Güvenli Oturum Katmanı), WEP (Wireless Equivalent Privacy, Kablosuz Denk Mahremiyet), WPA (Wireless Protected Access, Kablosuz Korumalı Erişim) gibi güncel pekçok uygulamada kullanılan **RC4**, bir **akış şifreleme** uygulamasıdır.

DİZİ ŞİFRELEME

RC4

- ❑ **RC4 algoritması şifrelenecek veriyi akan bir bit dizisi olarak algılar.**
- ❑ RC4 belirlenen anahtar ile veriyi şifreleyen bir algoritmadır.
- ❑ Genellikle hız gerektiren uygulamalarda kullanılır.
- ❑ **Şifreleme hızı yüksektir ve MB/sn seviyesindedir.**
- ❑ Güvenliği **rastgele bir anahtar kullanımına bağlıdır.**
- ❑ Anahtar uzunluğu değişkendir.
- ❑ **128 bitlik bir RC4 şifrelemesi sağlam bir şifreleme** olarak kabul edilir.
- ❑ **Bankacılık ve Dökümantasyon (PDF) şifrelemelerinde** yaygın olarak kullanılır.

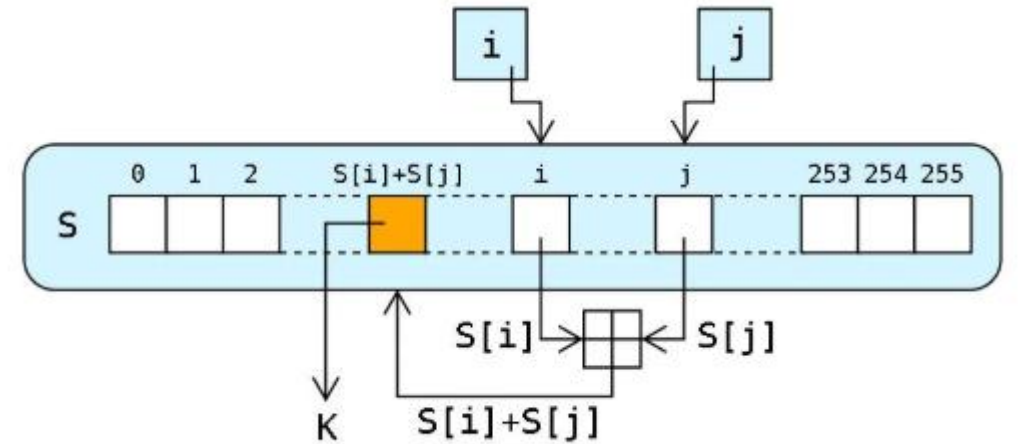
Roland Rivest, RSA, 1987

DİZİ ŞİFRELEME

RC4

RC4 algoritması, iki ana bileşene sahiptir:

1. Anahtar zamanlama algoritması (KSA): Bu algoritma, anahtarı kullanarak S-kutusunu oluşturur. S-kutusu, şifreleme ve şifre çözme için kullanılan rastgele bir dizidir.
2. Sözde rastgele üretim algoritması (PRGA): Bu algoritma, S-kutusunu kullanarak anahtar akışını oluşturur. Anahtar akışı, şifreleme ve şifre çözme için kullanılan rastgele bir dizidir.



RC4

Anahtar zamanlama algoritması (KSA):

KSA, 256 baytlık bir S-kutusu oluşturur. S-kutusu, 0'dan 255'e kadar olan sayılarla doldurulur. KSA, anahtarı kullanarak S-kutusunu şu şekilde oluşturur:

1. S-kutusunun her bir elemanına, dizinin indisine karşılık gelen değeri atar. Örneğin, $S[0] = 0$, $S[1] = 1$, $S[2] = 2$, ..., $S[255] = 255$.
2. Anahtardaki her bayt için, şu işlemleri gerçekleştirir:
 - "i" değişkenini anahtarın baytına eşitler.
 - "j" değişkenini 0 olarak ayarlar.
 - "S" ve "S[j]" değerlerini birbirleriyle değiştirir.
 - "[*]"j" değişkenini, $(j + S) \bmod 256$ olarak günceller.

RC4

Anahtar zamanlama algoritması (KSA):

PRGA, S-kutusunu kullanarak anahtar akışını oluşturur. Anahtar akışı, şifreleme ve şifre çözme için kullanılan rastgele bir dizidir. PRGA, anahtar akışını şu şekilde oluşturur:

- "i" ve "j" değişkenlerini 0 olarak ayarlar.
- Sürekli olarak, şu işlemleri gerçekleştirir:
 - ❖ "i" değişkenini, $(i + 1) \bmod 256$ olarak günceller.
 - ❖ "S" ve "S[j]" değerlerini birbirleriyle değiştirir.
 - [*]"t" değişkenini, $(S + S[j]) \bmod 256$ olarak ayarlar.
 - [*]"S[t]" değerini anahtar akışında bir bayt olarak çıkarır.

BLOK ŞİFRELEME



Dizi şifrelemeden farklı olarak **blok şifrelemede** açık metinler bloklar halinde şifrelenir.

- Her bir blok sırayla, simetrik algoritma kullanılarak şifrelenir.
- Elde edilen şifreli metinler yine aynı sırada çözülerek, açık metinler bloklar halinde elde edilir.
- Bu bloklar bir araya getirilerek orijinal metine ulaşılır.
- **Dizi şifrelemede** “merhaba” açık metni birer karakter şeklinde şifrelenirken, **blok şifrelemede** bu metin bütün olarak şifrelenebilir.

Blok şifreleme, iletilecek mesajı kullanılacak yöntemle ilgili olarak eşit uzunlukta parçalara ayırarak şifrelenmiş metne dönüştürür.

Dr. Fatih KALEMKUŞ

Klasik Şifreleme Algoritmaları

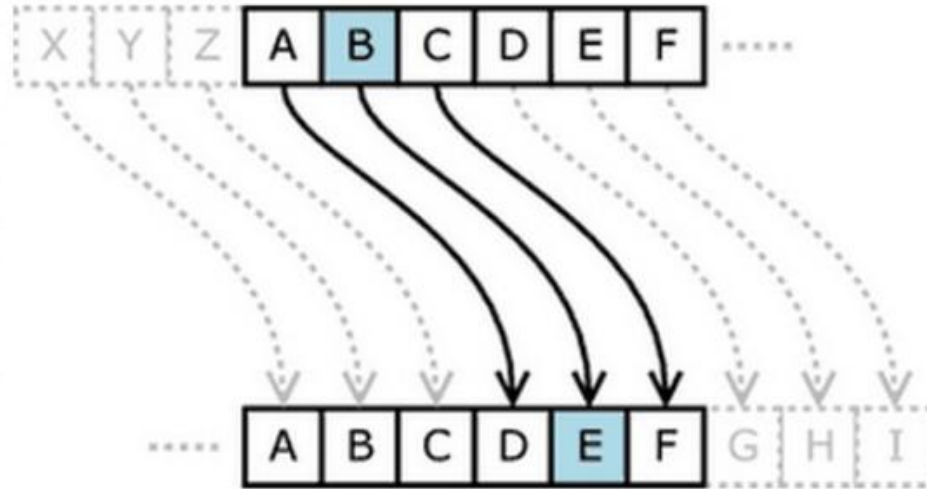
Günümüzde kullanılan modern şifreleme algoritmalarının yanında geçmiş zamanlarda kullanılmış ama şu an güvenilir kabul edilmeyen klasik şifreleme algoritmaları mevcuttur.

- Sezar Şifreleme Algoritması
- Affine Şifreleme
- Monoalfabetik Şifreleme
- Vigenere Şifreleme

Sezar Şifreleme Algoritması

Bilinen en eski şifreleme yöntemidir.

- Alfabe her harfin belirli sayıda karakter ötelenmesi ile şifreleme tablosu elde edilir.
- Şifrelenecek metin alfabede kendinden sonra gelecek 3. harfle yer değiştirilmektedir.



Affine Şifreleme

Sezar şifreleme yönteminin geliştirilmesiyle elde edilmiştir.

- Şifreleme işlemi için açık metin belirlenen bir sayı ile çarpılır.
- Daha sonra Sezar şifrelemesinde olduğu gibi öteleme miktarıyla toplanır.

Şifreleme fonksiyonu:

$$y = a * x + b \text{ mod } 26$$

Çözme fonksiyonu:

$$x = a^{-1} (y - b) \text{ mod } 26$$

Key

$$a = 5$$
$$b = 2$$

Plaintext

EBYU

Ciphertext

WHS

$$20 \times 5 + 2 = 102$$

$$102 = 24 \text{ (mod } 26 \text{)}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Monoalfabetik Şifreleme

- Sezar yönteminde kullanılan 26 farklı anahtar yeterince güvenlik sağlayamayacağını düşünür.
- Monoalfabetik şifrelemede anahtar uzayını artırmak için alfabedeki her bir karakter başka bir karakter ile değiştirilerek şifreleme tablosu oluşturulur.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	H	Z	U	X	I	C	P	O	Q	A	N	S	B	T	L	D	K	Y	R	E	J	G	W	F	V

Açık metnin “ankara” olması durumunda “MBAMKM” şifrelenmiş metni elde edilir.

Vigenere Şifreleme

Vigenere şifreleme algoritması, monoalfabetik yöntemleri çözmekte kullanılan sıklık analizi saldırılarına karşı olan zaafiyeti, şifrelenmiş metinde kullanılan her harfin neredeyse eşit sıklıkta kullanılmasıyla ortadan kaldırılmıştır.

- Bir parola vardır.
- Parola açık metinden kısa olması durumunda parola açık metin uzunluğunca tekrar edilir.
- Paroladaki her harf açık metindeki «A» karakterine karşılık gelir ve diğer karakterler Sezar şifrelemesinde olduğu gibi ötelenir.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

Tablo 3.4
Parolanın "ESKI" ve açık metnin 7 karakter uzunluğunda olması durumunda elde edilen Vigenere tablosu

Açık metin	A	N	A	D	O	L	U
Parola	E	S	K	I	E	S	K
Şifrelenmiş metin	E	F	K	L	S	D	E

Modern Simetrik Şifreleme Yöntemleri

Klasik şifreleme yöntemleri hesaplama gücünün yüksek olmadığı haberleşme ortamları için tercih edilebilir yöntemlerdir. Bilindiği gibi günümüzde hesaplama gücü yüksek bilgisayarlar sayesinde klasik yöntemlerle şifrelenen metinler kolaylıkla kırılabilir.

- Data Encryption Standard (DES)
- 3DES
- Advanced Encryption Standard (AES)
- International Data Encryption Algorithm (IDEA)
- Blowfish
- Cast-128
- IRON
- MD5
- SHA1

Veri Şifreleme Standardı (DES)

Data Encryption Standard (DES) IBM tarafından geliştirilen, Amerikan Ulusal Güvenlik Ajansı tarafından algoritmanın bazı adımlarında değişiklik yapılarak kabul edilen ve 1977-2001 yılları arasında yaygın kullanılan bir blok şifreleme algoritmasıdır.

- DES, 64-bit uzunluğunda bloklar kullanarak şifreleme yapar.
- 64 bitlik anahtar uzunluğu vardır ama 56 biti etkili şekilde kullanılır, geriye kalan 8 bit kontrol amaçlıdır.
- DES, 16 adet birbirinin aynısı işlemlerden oluşan turlardan meydana gelmektedir.

DES uzun yıllar boyunca güvenle kullanılmış ve üzerinde en çok araştırma yapılmış simetrik şifreleme algoritmalarından biridir.

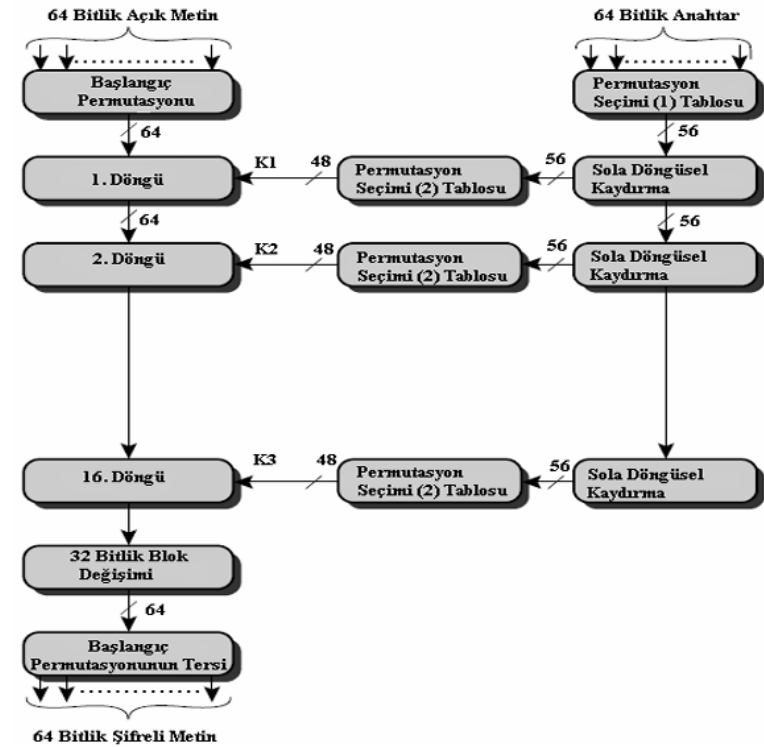
BLOK ŞİFRELEME

DES Algoritmasının Çalışma Prensibi

DES şifreleme algoritmasının çalışması prensibi şu şekildedir.

- İlk olarak data başlangıç permutasyonu olan IP (İnitial Permutation) de çalıştırılır,
- 64 bit'lik veri 32 bit'lik iki eşit parçaya ayrılır. Bunlar L (Left) ve R (Right) olarak adlandırılırlar. Başlangıç döngüsü olduğundan bu eşit parçalar L0 ve R0 diye adlandırılırlar.
- Bu döngü için oluşturulmuş alt anahtar f fonksiyonu kullanarak döngüye sokulur, ve bu döngü 16 kere tekrarlanır.
- 16 döngü sonrasında ayrılmış olan L ve R parçaları yerdeğıştir.
- Son olarak da döngüye sokulmuş olan 64 bitlik dataya IP'nin ters işlemini uygulanarak algoritma tamamlanır.

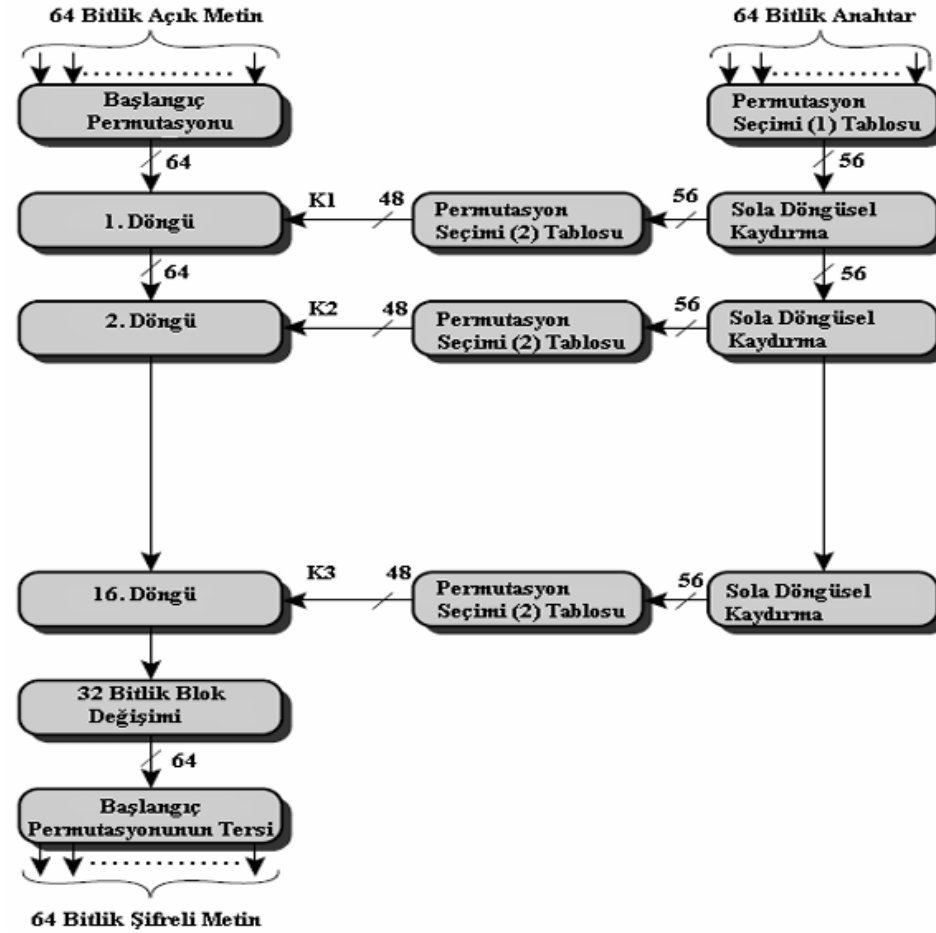
DES Şifreleme Algoritması Genel Blok Diyagramı



BLOK ŞİFRELEME

DES Şifreleme Algoritması Genel Blok Diyagramı

Örnek;



3DES

DES algoritmasının yaygın olarak bilinmesi ve kullanılmasından dolayı kaba kuvvet saldırılarına karşı koyabilecek alternatif çözümler ortaya konulmuştur. Bunlardan bir tanesi 3DES şifreleme yöntemidir.

- DES şifreleme algoritmasının 3 kez peş peşe farklı gizli anahtarlar kullanılarak uygulanmasıdır.
- Birinci seçenek gizli anahtarların üçünün de farklı seçilmesi durumudur ve $3 \times 56 = 168$ bitlik anahtar uzunluğuna karşılık gelir.
- DES şifrelemesine nazaran 3 kat ağır işler.
- DES algoritmasına göre daha güvenlidir.

BLOK ŞİFRELEME

3DES

Kuvvetli Tarafları:

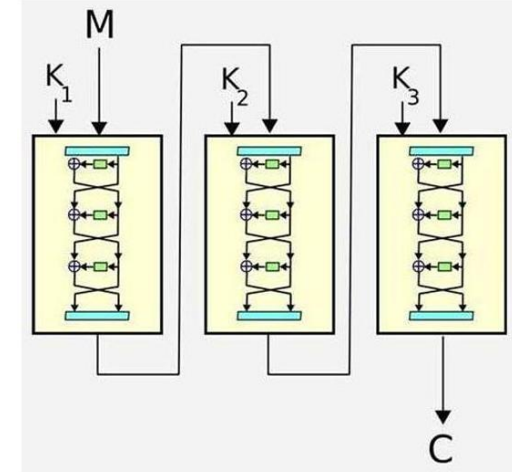
- İki yönlü çalışmasından dolayı veriler rahat bir şekilde saklanabilir ve dilediğinde tekrar çağırılarak data tekrar çözülebilir.
- Kullanılan cihazların (bilgisayarın) eksikliklerini giderir.

Zayıf Tarafları:

- Kullanılan anahtar sistemin güvenliğini oluşturur. Kullanılan anahtar ne kadar zayıfsa, şifrenin kırılması o kadar kolaydır.
- Günümüz teknolojisinde kullanılan daha gelişmiş AES algoritmasına nazaran 6 kat ağır işler.

Kullanım Alanları:

- Finans sektörü (bankacılık)
- Önemli güvenlik faaliyetlerinde
- İnternet üzerinden alışverişlerde (e-ödeme)



Şekil 5. 3DES Algoritmasının Akış Diyagramı

Gelişmiş Şifreleme Standardı (AES)

AES (Advanced Encryption Standard- Gelişmiş Şifreleme Standartı) ortaya çıkışı; DES algoritmasında kullanılan anahtar uzunluğunun kaba kuvvet saldırılarına karşın yetersiz kalması ve hem yazılım hem de donanım ortamında verimli şekilde çalışacak modern bir şifreleme algoritmasına ihtiyaç duyulması nedeniyle, **1997 yılında Birleşmiş Milletler Ulusal Standartlar ve Teknoloji Enstitüsü** bir yarışma çağrısı yaptı.

- Belçikalı bilim adamının geliştirdiği Rijndael birinci oldu ve gelişmiş şifreleme standardı (AES) olarak kabul edildi.
- AES algoritması SSH, IpSec, TLS ve Skype gibi güvenliğin önemli olduğu birçok protokolde kullanılmaktadır.
- AES algoritması 128, 192, 256 bit olmak üzere 3 farklı anahtar uzunluğu kullanarak 128 bitlik bloklar halinde şifreleme yapar.

Gelişmiş Şifreleme Standardı (AES) Döngü Yapısı

AES algoritmasında her döngü dört katmandan oluşur. AES algoritmasının genel yapısında giriş, çıkış ve matrisler 128 bitlidir. Bu matrisler 4 satır ve 4 sütun (4x4) olmak üzere 16 bölmeden meydana gelir. Oluşan bu matrise 'durum' denilmektedir. Durumun her bir bölmesinde birer byte veri vardır. Şifrelemede ilk önce 128 bitlik veri 4x4 byte'lık matrise dönüştürülür. Sonrasında sırasıyla her döngüde;

- Byte'ların yerdeğiştirilmesi,
- Satırların ötelenmesi,
- Sütunların karıştırılması ve
- Planlanan anahtar için o döngünün anahtarı XOR'lama işlemleri yapılır.

Byte'lar yerdeğiştirirken oluşturulan 16 byte 8 bit'i giriş ve 8 bit'i de çıkış olmak üzere S kutusuna gönderilir. S-kutusundaki değerler, Galois cisminde (Galois Field-GF) GF (28), 8 bitlik polinom için ters alındıktan sonra lineer bir dönüşümle oluşturulmuştur. Satırların ötelenmesi işlemi ise 16 bölümden oluşan matrisdeki satırlar ötelenir ve sütunların karıştırılması işlemi ise sütunlar kendi içinde karıştırılır. Son aşamada ise oluşturulan döngü anahtarı XOR'lama yapılarak işlem sonlandırılır. (XOR veriler anahtar bilgileri ekler)

Gelişmiş Şifreleme Standardı (AES)

AES anahtar uzunluğuna bağlı olarak birbirinin benzeri turlardan oluşmaktadır.

Anahtar uzunluğu	Tur sayısı
128	10
192	12
256	14

*Tablo 3.5
AES anahtar uzunluğu
ve tur sayıları*

AES şifreleme algoritmasının turları üç temel işlemde oluşmaktadır:

- **Anahtar ekleme katmanı:** Tur anahtarı ile durum matrisi XORlanır
- **Bayt yer değiştirme katmanı:** Durum matrisi S-Box adı verilen doğrusal olmayan bir tablo ile dönüştürülür.
- **Yayıma katmanı**
 - **Satır kaydırma katmanı (ShiftRows):** Durum matrisindeki satırlar dairesel olarak belirli sayıda kaydırılır.
 - **Sütun karıştırma katmanı (MixColumn):** Durum matrisinin sütunları karıştırılır.

Uluslararası Veri Şifreleme Algoritması (IDEA)

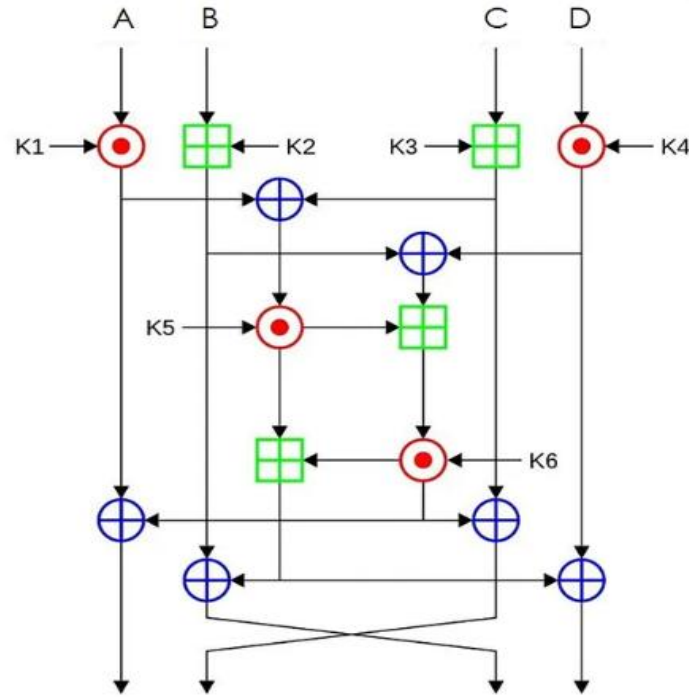
DES, 3DES ve AES simetrik şifreleme algoritmalarına ek olarak kullanılan bir diğer simetrik şifreleme algoritması **International Data Encryption Algorithm (IDEA)** olarak adlandırılır.

- 1991 yılında Xuejia Lai ve James L. Massey tarafından geliştirilmiştir.
- 64 bitlik açık metin 16 bitlik dört bloğa ayrılarak, 16 bitlik bloklar halinde şifrelenir.
- IDEA çalışma şekli bakımından diğer simetrik algoritmalara benzemektedir.
- Özellikle DES ile birbirlerine çok benzerler.

BLOK ŞİFRELEME

IDEA Şifreleme Diyagramı

Düz metnin dört bölüme ayrılır: A, B, C ve D. Ayrıca K(1) ila K(52) adlı 52 alt anahtar verilmiş olsun.



- ❑ 64 bit veri bloğu giriş ve çıkış için kullanılır,
- ❑ Her turda 6 anahtar kullanır,
- ❑ 3 matematiksel fonksiyona dayalıdır:

 : Toplama
($\text{Mod } 2^{16}$)

 : Çarpma
($\text{Mod } 2^{16} + 1$)

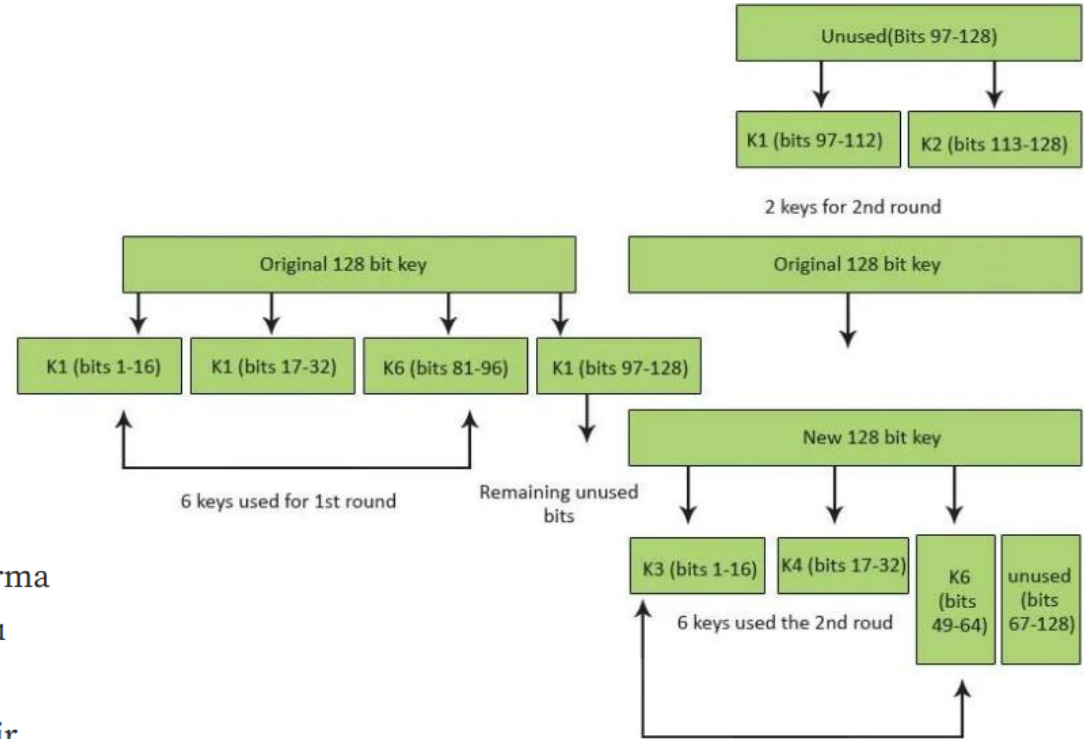
 : Xor İşlemi

- ❑ Toplam 8.5 tur işlem içerir

Şekil 1: IDEA İşleyişi (İlk döngü ve genel bilgiler)

IDEA Şifrelemenin Anahtar Üretimi

IDEA'nın 128 bit anahtarı, ilk sekiz alt anahtar 16 bit olarak, K(1) ila K(8) arasında alınır. Sonraki sekiz alt anahtar, 25 bitlik dairesel bir sola kaydırma işleminden sonra aynı şekilde elde edilir ve tüm şifreleme alt anahtarları elde edilene kadar bu tekrarlanır. Bu, toplamda 6 tur boyunca ortalama olarak bir turda bir kereden daha az döndürüldüğü anlamına gelmektedir.



Şekil 2: IDEA'nın Anahtar Üretimi

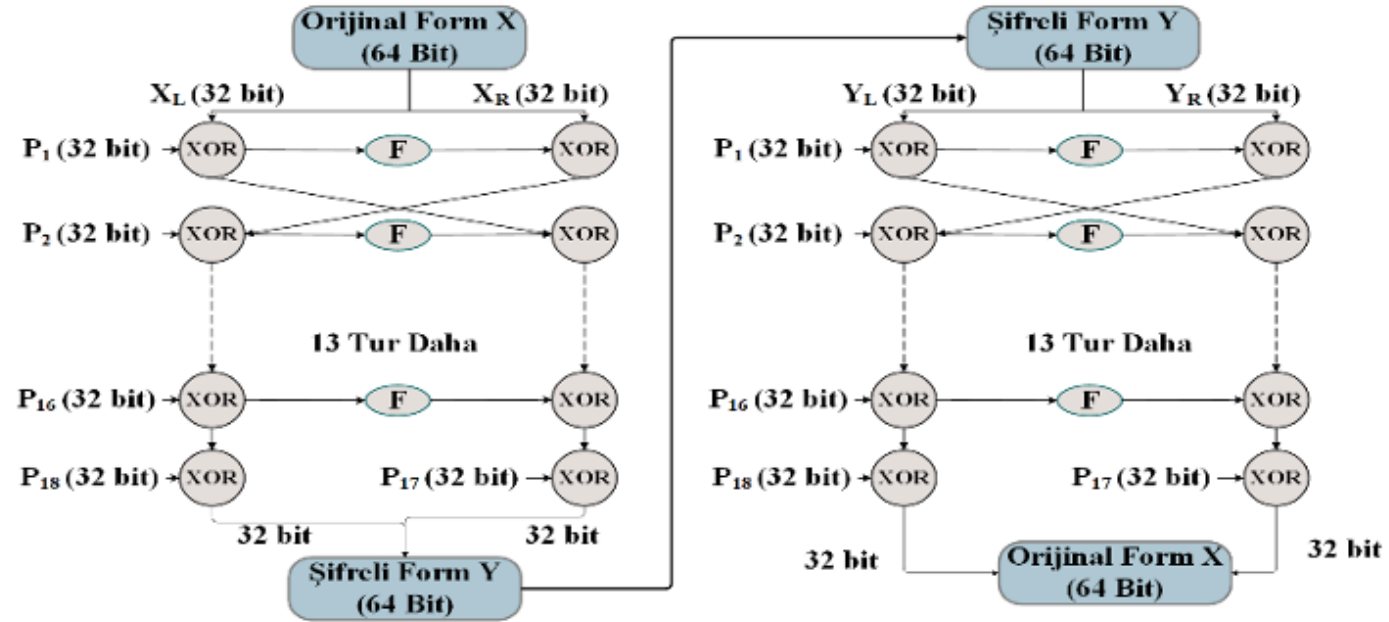
Blowfish

Anahtar uzunluğu (32- 448 bit arasında değişen) esnek ve DES' ten daha hızlı yapısıyla Blowfish algoritması, 64 bitlik bloklara mesajları bölerek kodlama yapmaktadır.

- 64 bitlik bloklar, anahtar ve veri genişletmeye bölünerek çalıştırılır.
- Kendine özgü diğer avantajlar (karmaşık tuş programı, verimlilik, yüksek hız ve bağımsız S kutuları gibi) sayesinde Blowfish en hızlı algoritmalarından biri konumundadır.
- Güvenlik riski taşıyan durumlarda anahtarın aktarılmasındaki hassasiyet, zaman faktöründeki tüketim hacmi gibi vb. durumlar algoritmanın dezavantajlarıdır.

Blowfish

Blowfish
kriptografik süreci
Şekil 5 ile
görselleştirilmiştir.

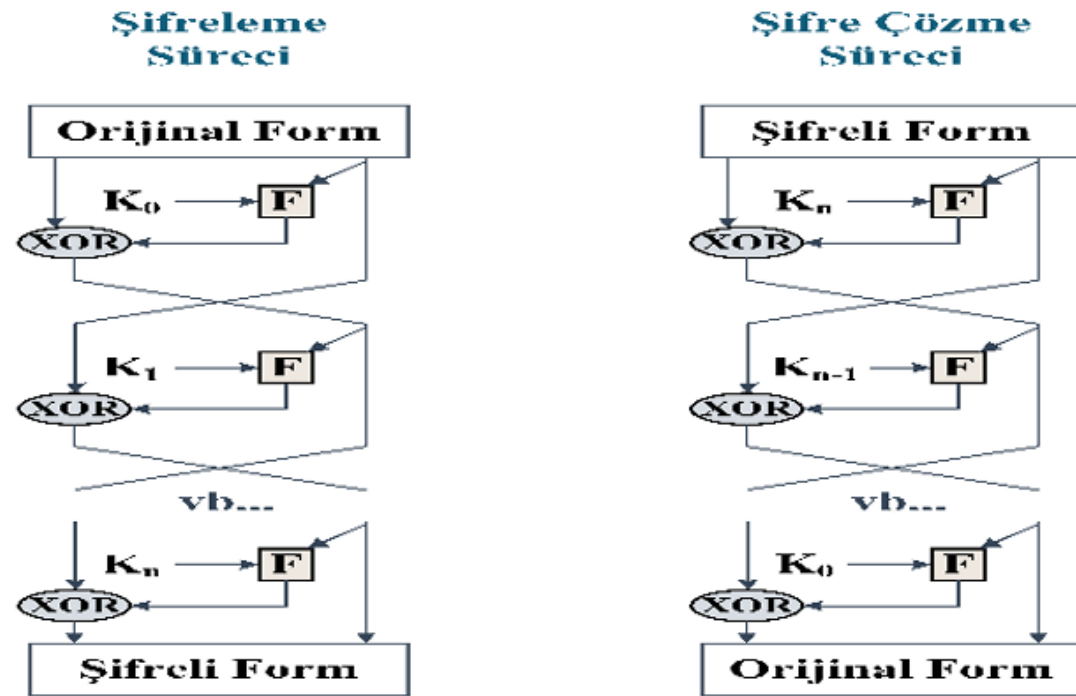


Şekil 5. Blowfish kriptografik süreci

BLOK ŞİFRELEME

Cast-128

Anahtar uzunluğu 8 bit artışla 40- 128 bit aralığında değişen Cast-128, 64 bitlik düz metin şablonunu 64 bitlik kodlanmış forma dönüştürürken 16 döngülük yapıyla çalışmaktadır.



Twofish

- Twofish, Counterpane Labs tarafından 1998 yılında yayınlanan bir blok şifresidir.
- Beş Gelişmiş Şifreleme Standardı (AES) finalisti arasındaydı ve **AES olarak seçilmedi**.
- Twofish, 128 bitlik bir blok boyutuna, 128 ila 256 bit arasında değişen bir anahtar boyutuna sahiptir ve 32 bitlik CPU'lar için optimize edilmiştir.

IRON

- IRON, 64 bitlik veri bloklarını 128 bitlik anahtarla şifrelemede kullanılır.
- Döngü (round) sayısı 16 ile 32 arasındadır.
- Sanal verilerin saklandığı Flash sürücülerde güvenliği artırmak için kullanılır.

MD5 (Message-Digest Algorithm 5)

Message Digest 5 (MD5) algoritması, verilen dosyanın veya mesajın (şifre vb.) kendine has "parmak izi" nin oluşturulmasını "hash" fonksiyonlarına dayalı olarak sağlayan bir algoritmadır. Bir veritabanı yönetimi (database management) tekniğidir. 1991 yılında MIT (Massachusetts Institute of Technology)'de görev yapan Profesör Ron Rivest tarafından geliştirilmiştir. Profesör Rivest MD5'i MD4'ün bir üst sürümü olarak tasarlamıştır.

MD5 (Message-Digest Algorithm 5)

Özellikleri:

- MD5 algoritması tek yönlü çalışır. Şifreleme yapılır, ancak şifre çözüm işlemi yapılamaz.
- MD5 algoritması, üzerinde işlem yapılan dosyada (aktarma vb.) herhangi bir değişiklik olup olmadığını tespit eder. Eğer bir değişiklik yapılmışsa, yeni dosyanın MD5 algoritmasından geçilmesinden çıkan sonuç ile ilk dosyanın MD5 sonucu birbirinden farklı olacaktır.
- MD5 algoritması bir alt sürümü olan MD4'e göre yavaş çalışır, ancak şifreleme sistemi çok daha karışık ve çözülmesi güçtür.
- Genel olarak 4 farklı aşamalı bir sisteme sahiptir. Her aşama birbirinden farklı işleyişe sahip olup 16'şar basamaktan oluşmuştur.
- Boyutu fark etmeksizin algoritmaya girişi yapılan dosyanın çıkışı olarak 128-bit uzunluğunda 32 karakterli 16'lık sayı sisteminde bir dizi elde edilir.

Kullanıldığı Yerler:

- İnternet trafiğinde. "SSL (Secure Sockets Layer - Güvenli Yuva Katmanı)" gibi.
- Özel bilgisayar ağlarında. "VPN (Virtual Private Network - Sanal Özel Ağ)" gibi.
- Güvenli uzaktan ulaşım uygulamalarında. "SSH (Secure Shell - Güvenli Kabuk)" gibi.
- Kimlik belirleme uygulamalarında.

MD5 (Message-Digest Algorithm 5)

Dezavantajları:

- Kullanıcı adı ve şifre ile giriş yapılan sitelerde, kullanıcı şifresini unuttuğu takdirde sistem eski şifreyi veremez. Şifre, MD5 algoritmasından geçirilmiş halde saklandığı için şifre çözülemez. Sistem kullanıcıya yeni şifre atar.
- MD4 'e göre daha uzun bir şifre ürettiğinden çalışması daha uzun zaman alır.
Çakışmalar (Collisions)

SHA1 (Secure Hash Algorithm – Güvenli Özetleme Algoritması)

Secure Hashing Algorithm olarak adlandırılan, şifreleme algoritmaları içerisinde en yaygın olarak kullanılan algoritma olduğu kabul gören SHA1, United States National Security Agency tarafından tasarlanmıştır. “Hash” fonksiyonlarına dayalı veritabanı yönetimine (database management) imkan sağlar.

Özellikleri:

- SHA1 algoritması ile sadece şifreleme işlemi yapılır, şifre çözümü işlemi yapılamaz.
- Diğer SHA algoritmaları içerisinde en yaygın olarak kullanılan SHA1 algoritmasıdır.
- SHA1 algoritması ile 160 bitlik özetler oluşturulur. MD5 ve SHA1 arasındaki temel fark oluşturdukları özetlerdeki boyut farkıdır.
- SHA1 algoritması, e-posta şifreleme uygulamaları, güvenli uzaktan erişim uygulamaları, özel bilgisayar ağları ve daha birçok alanda kullanılabilir.
- Günümüzde güvenliği arttırmak amacıyla SHA1 ve MD5 algoritmaları birbiri ardına kullanılarak veriler şifrelenir.

Blok Şifreleme Metotları

- **Elektronik Kod Kitabı (Electronic Code Book-ECB):** Açık metni kullanıla goritmaya göre uygun uzunluktaki bloklara böler. Her bir bloğu bağımsız şekilde gizli anahtar kullanarak şifrelenmiş metin elde eder.
- **Şifre Blok Zincirleme (Cipher Block Chaining -CBC):** CBC mod hem üretilecek şifrelenmiş metnin kendisinden önceki bütün açık metinlere bağılı olmasını, hem de şifreleme yöntemini ilk turda rastgele sayılardan oluşturulan bir vektör kullanarak farklılaştırmayı amaçlar.
- **Çıktı Besleme Modu (Output FeedBack Mode-OFM):** Bu mod dizi şifreleme algoritmalarında kullanılır.
- **Sayaç Modu (Counter Mode-CM):** OFM moda benzerdir. Şifreleme algoritmasına başlangıç vektörünün sonuna ilk tur için 1 sayısı eklenerek gönderilir ve diğer turlarda bu sayı artırılır.
- **Şifre Geri Besleme Modu (Cipher FeedBack Mode-CFB):** İlk tur hariç diğer bütün turlarda üretilen şifrelenmiş metin, şifreleme algoritmasına girdi olarak gönderilir. Şifreleme algoritmasının çıktısı ile açık metin XOR'lanır.

SİMETRİK ŞİFRELEME

Güçlü ve Zayıf Yönleri

Kuvvetli Yönleri;

- Algoritmalar olabildiğince hızlıdır.
- Donanımla birlikte kullanılabilir.
- “Gizlilik” güvenlik hizmetini yerine getirir.
- Anahtarın boyu ve dolayısıyla bit sayısı çok daha küçüktür.

Zayıf Yönleri;

- Güvenli anahtar dağıtımı zordur.
- Kapasite sorunu vardır.
- Kimlik doğrulama ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek zordur.

Sorular



Dr. Fatih KALEMKUŞ



TEŞEKKÜRLER

Dr. Fatih KALEMKUŞ