Kriptosistemler ve Şifreleme Yöntemleri

Kriptoloji

- Kryptos logos”, “gizli”, “dünya”
- Haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor ifadelere dayanan tekniklerin ve uygulamaların bütünüdür.
- “Matematik, elektronik, optik, bilgisayar, sosyal mühendislik bilimleri gibi bir çok disiplini kullanan özelleşmiş bir bilim dalı”

Kriptoloji

Kriptografi

- Belgelerin şifrelenmesi ve şifrelerinin çözülmesi için kullanılan yöntemlere verilen addır.
- **Kriptoanaliz**

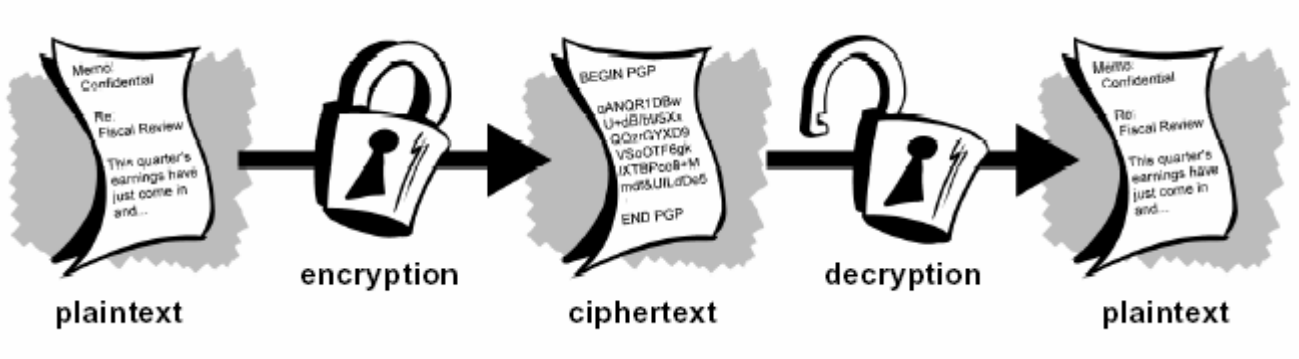
Kriptografik sistemlerin kurduğu mekanizmaları inceler ve çözmeye çalışır.

Kriptosistemler

- Kimlik doğrulama ve şifreleme verinin güvenliğini sağlamaya yarayan birbiriyle bağlantılı iki teknolojidir.
- Kimlik doğrulama, haberleşmede her iki tarafta bulunanların ne söylüyorlar ise onun doğru olmasını sağlama sürecidir. Bir mesajın bütünlüğü ve güvenilirliği tek yönlü hash fonksiyonunun ve sayısal imzanın kullanılmasını gerektirir.
- Şifreleme ise iletişim sırasında verinin hem güvenliğini sağlamak hem de değiştirilmesini önlemeye yönelik işlemlerdir. Değişik Şifreleme algoritmaları kullanılarak yapılır.

Şifreleme Nedir?

- Bir açık metinin bir şifreleme algoritması yardımıyla anlaşılamaz hale getirilmesi işlemine şifreleme denir.



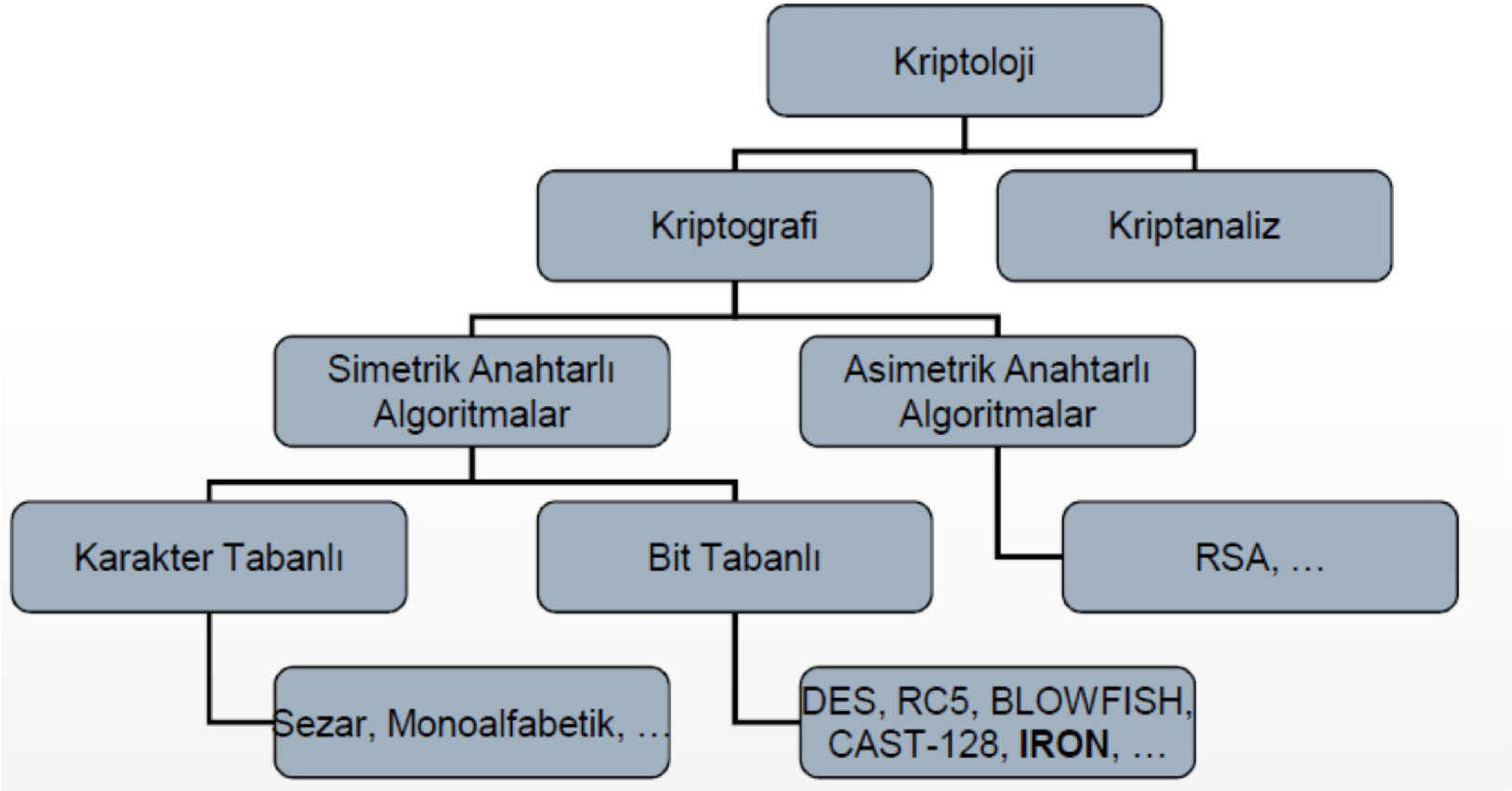
Şifreleme Nedir?

- Şifrelenecek mesaj plaintext (düz-metin) olarak adlandırılır.
- Şifreleme(encryption); veriyi alıcının haricinde kimse okuyamayacak şekilde kodlamaktır.
- Şifrelenmiş mesaja ciphertext (şifreli-mesaj) denir
- Şifre Çözme(Decryption) ise şifrelenmiş veriyi çözüp eski haline getirme işlemidir.
- Veriyi şifrelerken ve çözerken kullanılan matematiksel metoda ise şifreleme algoritması denilmektedir.
- Şifreleme ve çözme genelde bir anahtar(Key) kullanılarak yapılır

Şifreleme Algoritmalarının Performans Kriterleri

- Kırılabilme süresinin uzunluğu.
- Şifreleme ve çözme işlemlerine harcanan zaman (Zaman Karmaşıklığı).
- Şifreleme ve çözme işleminde ihtiyaç duyulan bellek miktarı (Bellek Karmaşıklığı).
- Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği.
- Bu uygulamaların dağıtımındaki kolaylık yada algoritmaların standart hale getirilebilmesi.
- Algoritmanın kurulacak sisteme uygunluğu.

Algoritmaların genel tasnifi



Şifreleme Algoritmaları

- Kriptografide şifreleme için kullanılan anahtarın özellikleri ve çeşidine göre temel olarak iki çeşit şifreleme algoritması bulunmaktadır.
  - Simetrik şifreleme algoritmaları
  - Asimetrik şifreleme algoritmaları

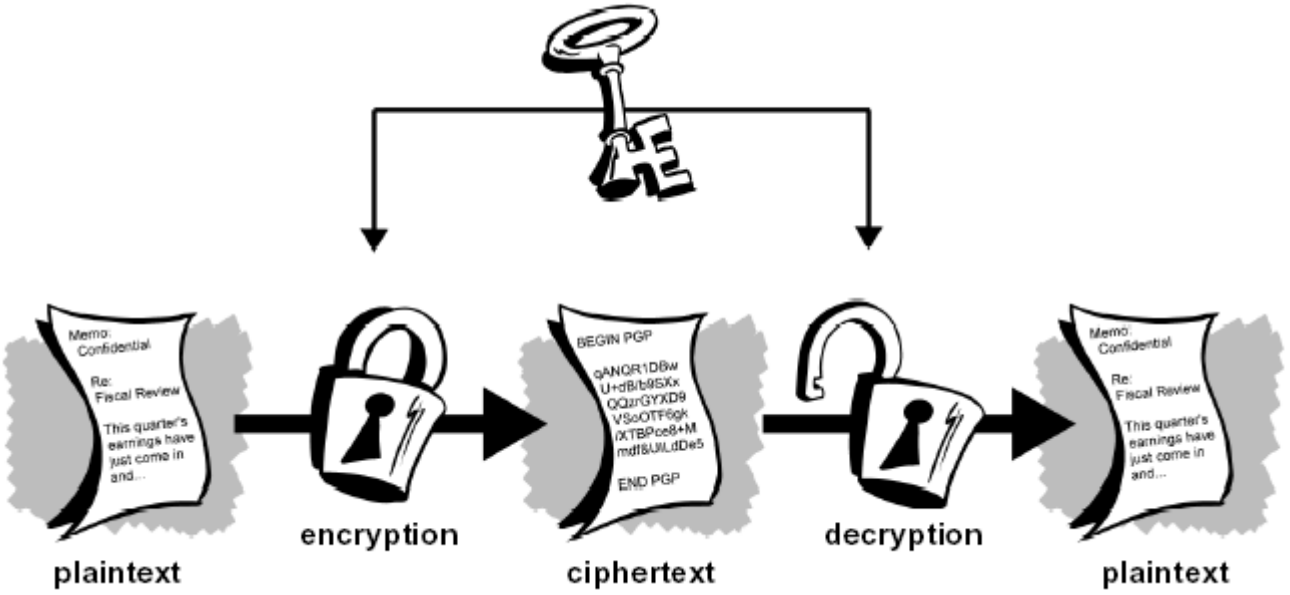
Simetrik Şifreleme Algoritmaları

- Bu algoritmada şifreleme ve şifre çözmek için bir tane gizli anahtar kullanılmaktadır.
- Kullanılan anahtar başkalarından gizlidir ve şifreleme yapan ile şifrelemeyi çözecek kişilerde arasında anlaşılmış ortak bir anahtardır.
- Gönderilecek gizli metinle beraber üstünde anlaşılmış olan gizli anahtar da alıcıya gönderilir ve şifre çözme işlemi gerçekleştirilir.

Simetrik Şifreleme Algoritmaları

- Simetrik şifrelemenin en önemli avantajlarından birisi oldukça hızlı olmasıdır.
- Asimetrik şifrelemeyle karşılaştırıldığında hız konusunda simetrik algoritmalar çok daha başarılıdır.
- Bununla birlikte simetrik algoritmayı içerdiği basit işlemlerden dolayı elektronik cihazlarda uygulamak çok daha kolaydır.
- Ayrıca simetrik algoritmalarda kullanılan anahtarın boyu ve dolayısıyla bit sayısı çok daha küçüktür.

Simetrik Şifreleme Algoritmaları



Simetrik Şifreleme Algoritmaları

- Kuvvetli Yönleri;
  - Algoritmalar olabildiğince hızlıdır.
  - Donanımla birlikte kullanılabilir.
  - Güvenlidir.
- Zayıf Yönleri;
  - Güvenli anahtar dağıtımı zordur.
  - Kapasite sorunu vardır.
  - Kimlik doğrulama ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek zordur.

Simetrik Şifreleme Yöntemleri

Karakter tabanlı simetrik şifreleme yönt.

- Basit Şifreleyiciler (Metni ters çevirmek v.b)
- Ötelemeli Şifreler (Sezar Şifresi)
- Tek Alfabede Yerine Koymalı Şifreler
- Çok Alfabeli Yerine Koymalı Şifreler
- Tek Kullanımlı Şifreler

Günümüzde Kullanılan Simetrik Şifreler

BASİT ŞİFRELEYİCİLER (Cipherlar)

Normal yazılışlı harfleri değiştirme operasyonunu kapsar

- Metni ters çevirmek (Message Reversal)
- Geometrik yöntemler (Geometrical Patterns)
- Yolu değiştirme (Route Transposition)
- Yol değişiklikleri (Route Variations)
- Dikey değiştirme (Columnar Transposition)
- Dikey değiştirme yöntemi (Other Transposition)
- Çifte dikey değiştirme (Double Columnar Transposition)
- Çok harfli değiştirme (Poly Literal Transposition)
- İşaret sözcüğünün değiştirilmesi (Code Word Transposition)

Metni Ters Çevirme (Message Reversal)

- Düz bir metni basit olarak şifrelemek için kullanılır.
- Düz metin tersten yazılır.

- *"Gazi Üniversitesi"* tersi yani *"isetisrevinü izaG"* şifreli metin elde edilir.

- Tersiyle düz metin elde edilir.

Geometrik Yöntemler (Geometric Patterns)

- Düz metin soldan sağa ve satır satır yazılır.
- Böylece mesajlar dikdörtgen şeklinde oluşturulur.

Örnek: "GAZİ ÜNİVERSİTESİ"

(1) Düz metin dikey iki sütün halinde yazabiliriz:
GE
AR
ZS
İİ
ÜT
NE
İS
Vİ
Düz metin yatay olarak eşit uzunlukta iki satır halinde yazılır:
(2) GEAR ZSİİÜTNEİSVİ

Yol Değiştirme (Route Transposition)

- Yolu değiştirme metodu ek karıştırma sağlar.
- Soldan sağa yazma yolunu kullanırsa

Örneğin: (16 Karakter) (8x2 matris oluşturulur.)

GAZİ ÜNİVERSİTESİ (Düz Metin)

GA
Zİ
ÜN
İV
ER
....

- GZÜİEG.. AİNVR.. (Şifreli Metin)

Columnar tranposition (Sütün yerdeğiştirme) şifreleme yönteminde amaç karakterlerin kimliklerini değiştirmeden pozisyonlarını değiştirmektir. **Şifre kullanılarak** veya sadece **satir sütün** değişikliği yapılarak uygulanabilir. Columnar transposition şifreleme yönteminde bir C değeri ile şifrelenecek metin tabloya sokulurken tabloda olacak sütün sayısı belirlenir. Aşağıdaki örnek için C=5 alınmıştır.

Dikey Değiştirme (Columnar Transposition)

- **Dikey değişiklik yapılır**
- **Düz metin dikdörtgen şekline getirilir ve dikey metot uyg**

"SHIP EQUIPMENT ON THE FOURTH OF JULY"

Sütun numarası

1	2	3	4	5
S	U	T	F	O
H	I	O	O	F
I	P	N	U	J
P	M	T	R	U
E	E	H	T	L
Q	N	E	H	Y

C=5 içinŞifreli metin: Anahtarsız şifreleme için

SUTFOHIOOFIPNUJPMTRUEEHTLQNEHY

C=5 ve YOBGE anahtarı (şifresi) için

‘ SHIP EQUIMPMENT On THE FOURTH OF JULY’ metnini şifreleyelim..

Orijinal 5 sütünlu dönüşüm

Sütun numarası				
1	**2**	**3**	**4**	**5**
S	U	T	F	O
H	I	O	O	F
I	P	N	U	J
P	M	T	R	U
E	E	H	T	L
Q	N	E	H	Y

1-YOBGE şifresinin harflerinin alfabe sıra numarası

Y	O	B	G	E
5	4	1	3	2

1	**2**	**3**	**4**	**5**
S	U	T	F	O
H	I	O	O	F
I	P	N	U	J
P	M	T	R	U
E	E	H	T	L
Q	N	E	H	Y

2- Şifre harf sırasına göre düzenleme

B	E	G	O	Y
1	2	3	4	5

3	**5**	**4**	**2**	**1**
T	O	F	U	S
O	F	O	I	H
N	J	U	P	I
T	U	R	M	P
H	L	T	E	E
E	Y	H	N	Q

Şifrelenmiş metin

TOFUSOFOIHNJUPITURMPHLTEEEYHNQ

Alıcıya gelen Şifreli metin: **TOFUSOFOIHNJUPITURMPHLTEEEYHNQ**
metninin C=5 ve YOBGE anahtarına göre deşifre edilmesi

1- Bu metin C=5'e göre düzenlenirse;

B	E	G	O	Y
1	2	3	4	5
T	O	F	U	S
O	F	O	I	H
N	J	U	P	I
T	U	R	M	P
H	L	T	E	E
E	Y	H	N	Q

2- Daha sonra şifre kelimesine göre düzenlenir.

Y	O	B	G	E
5	4	1	3	2
1	**2**	**3**	**4**	**5**
S	U	T	F	O
H	I	O	O	F
I	P	N	U	J
P	M	T	R	U
E	E	H	T	L
Q	N	E	H	Y

Buradan; sütunlardan orijinal metin elde edilir.

SHIP EQUIPMENT ON THE FOURTH OF JULY

Dikey Değiştirme (Columnar Transposition)

Açık metin:

Negotiations stalles send instructions today

Düz metin, dört sütun şeklinde:

N	N	E	T
E	S	N	I
G	S	D	O
O	T	I	N
T	A	N	S
I	L	S	T
A	L	T	O
T	E	R	D
I	D	U	A
O	S	C	Y

Çifte Dikey Değiştirme (Double Columnar Transposition)

- Anahtarın birinci numarasını (4213) kullanarak aşağıdaki düz metin değiştirilir.

Sütun yerleri anahtarı

1	2	3	4
4	2	1	3
T	N	N	E
I	S	E	N
O	S	G	D
N	T	O	I
S	A	T	N
T	L	I	S
O	L	A	T
D	E	T	R
A	D	I	U
Y	S	O	C

- Anahtarın ikinci numarasını (5926) kullanarak aşağıdaki sütunların değişmesi sağlanır.

Sütun yerleri anahtarı

5	9	2	6
2	4	1	3
N	E	T	N
S	N	I	E
S	D	O	G
T	I	N	O
A	N	S	T
L	S	T	I
L	T	O	A
E	R	D	T
D	U	A	I
S	C	Y	O

Ötelemeli Şifreleme (K=3 ise Sezar Şifresi)

2000 yıldan daha uzun bir zaman önce Sezar tarafından geliştirilen bu yöntem S= (*x+K)* mod(29) şeklindedir.

eK(x) = (x+ K) mod (26) *(Şifreleme)*

dK(y) = (y- K) mod (26) *(Deşifreleme)* $(x , y \in Z_{29})$

Örneğin:

S= x+3 mod(29)

A B C Ç D E F G Ğ H I İ J K L M N O Ö P R S Ş T U Ü V Y Z

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

Her harf kendinden sonraki 3. Harf ile şifrelenir.

T Ü R K İ Y E

V Z T N L B Ğ

TEK ALFABEDE YER DEĞİŞTİRME (YERİNE KOYMALI) ŞİFRELEME

Yer değiştirme (yerine Koyma) şifresinde şifreleme ve deşifreleme alfabetik karakterlerin permütasyonu şeklindedir.

P=C =Z_{26} olsun. K , 26 sembolün 0, 1, 2, ... , 25 tüm mümkün permütasyonlarını içerir.

Her permütasyon π ∈ *K için*

eπ(x) = π(x) (Şifreleme)

dπ(x) = π-1 (x) (Deşifreleme)

Burada π-*1 , π'nin tersi permütasyonudur.*

Tek Alfabede Yerine Koymalı Şifreler

A={A,B,C,...,V,Y,Z} açık metin alfabesi ve

B={MCRKHATL...GÜJV} şifreli metnin alfabesi olsun;

İki kümenin elemanları birebir eşlendiğinde:

T-Ü-R-K-İ-Y-E açık metni, Ç-Ğ-Ö-G-E-J-A şifrelenmiş metnine dönüşür. Alfabe kümesinin eleman sayısı 29 olduğu için; 29! kadar farkı alfabe türetmek olasıdır.

Aşağıda rasgele permütasyon π'nin bir örneği (Anahtar) görülmektedir. (Açık metin karakterleri küçük harfle, şifreli metin karakterleri büyük harfle yazılmıştır.)

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

Çok Alfabeli Yerine Koymalı Şifreler

A = {ABCÇDEFGĞHIİLKLMNOÖPRSŞTUÜVYZ} açık metin alfabesi

B_1= {MCRKHATLNBDEFGIZHOYSÖUŞÇİĞÜJV}

B_2= {JBEDFKCMRNLİÇTÜAVHZOIGYSUÖŞPĞ}

B_3= {BĞVTÜARFEDKÖLGÇCMUPNİHIYSZOŞJ}

şifreli metin alfabeleri olsun.

DİSKET açık metninin şifrelenmiş hali HİHGKY olur

En yaygın çok alfabeli yerine koyma şifresi **Vigenere'** dir. Bu şifreleme yönteminde 26' ya 26 hücreden oluşan İngiliz alfabesindeki harflere göre düzenlenmiş hali kullanır . Bu tablo kullanılarak yapılan şifreleme işleminde açık metin harfleri tablonun en üst satırında, anahtar harfler de tablonun en sol sütununda aranır. Açık metin harflerine karşılık gelen anahtar kelimenin harflerinin kesişmesi ile şifreli metine ulaşılır. Örnek olarak **CIPHER** anahtar kelimesini kullanarak şifreleme işlemini gerçekleştirelim.

Açık Metin: DONT TELL ANYONE
Anahtar: C I PH ERCI PHERCI
Şifreli metin: FWCA XVNT PUCFPM
Açık metin harflerini ilk satırdan anahtar kelimenin harflerine ait alfabeyi de sol sütundan çıkartalım.

A-> ABCDEFGHIJKLMNOPQRSTUVWXYZ
C-> CDEFGHIJKLMNOPQRSTUVWXYZAB
I-> IJKLMNOPQRSTUVWXYZABCDEFGH
P-> PQRSTUVWXYZABCDEFGHIJKLMNO
H-> HIJKLMNOPQRSTUVWXYZABCDEFG
E-> EFGHIJKLMNOPQRSTUVWXYZABCD
R-> RSTUVWXYZABCDEFGHIJKLMNOPQ

Deşifrelemede ise şifrelemedeki işlemin tersine şifreli metindeki harfler anahtar kelimenin harfleri ile kesiştirilip açık metine ulaşılır.

Vigenere tablosu

- Bu yöntemde oluşturulan tablo ve bir anahtar kelime kullanılarak şifreleme yapılır.

- Şifreleme
- Açık Mesaj (sütun) : BULUŞ MAYER İANKA RA
- Anahtar Kelime (satır): KALEM KALEM KALEM KALEM...
- Şifreli Mesaj : LUZAĞ ZAJIF UABÖM DA

- Şifre Çözme
- Şifreli Mesaj (tablo) : LUZAĞ ZAJIF UABÖM DA
- Anahtar Kelime (satır) : KALEM KALEM KALEM KALEM...
- Açık Mesaj (sütun) : BULUŞ MAYER İANKA RA

Tablo Türk Alfabesi Kullanılarak Oluşturulmuş Vigenere Tablosu

ABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZ
BCÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZA
CÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZAB
ÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZABC
DEFGĞHIİJKLMNOÖPRSŞTUÜVYZABCÇ
EFGĞHIİJKLMNOÖPRSŞTUÜVYZABCÇD
FGĞHIİJKLMNOÖPRSŞTUÜVYZABCÇDE
GĞHIİJKLMNOÖPRSŞTUÜVYZABCÇDEF
ĞHIİJKLMNOÖPRSŞTUÜVYZABCÇDEFG
HIİJKLMNOÖPRSŞTUÜVYZABCÇDEFGĞ
IİJKLMNOÖPRSŞTUÜVYZABCÇDEFGĞH
İJKLMNOÖPRSŞTUÜVYZABCÇDEFGĞHI
JKLMNOÖPRSŞTUÜVYZABCÇDEFGĞHIİ
KLMNOÖPRSŞTUÜVYZABCÇDEFGĞHIİJ
LMNOÖPRSŞTUÜVYZABCÇDEFGĞHIİJK
MNOÖPRSŞTUÜVYZABCÇDEFGĞHIİJKL
NOÖPRSŞTUÜVYZABCÇDEFGĞHIİJKLM
OÖPRSŞTUÜVYZABCÇDEFGĞHIİJKLMN
ÖPRSŞTUÜVYZABCÇDEFGĞHIİJKLMNO
PRSŞTUÜVYZABCÇDEFGĞHIİJKLMNOÖ
RSŞTUÜVYZABCÇDEFGĞHIİJKLMNOÖP
SŞTUÜVYZABCÇDEFGĞHIİJKLMNOÖPR
ŞTUÜVYZABCÇDEFGĞHIİJKLMNOÖPRS
TUÜVYZABCÇDEFGĞHIİJKLMNOÖPRSŞ
UÜVYZABCÇDEFGĞHIİJKLMNOÖPRSŞT
ÜVYZABCÇDEFGĞHIİJKLMNOÖPRSŞTU
VYZABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜ
YZABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜV
ZABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜVY

- Şifreleme
- Açık Mesaj (sütun) : BULUŞ MAYER İANKA RA
- Anahtar Kelime (satır) : KALEM KALEM KALEM KALEM...
- Şifreli Mesaj : LUZAĞ ZAJI F UABÖM DA

Tek Kullanımlık Karakter Dizisi (One-time Pad)

- Bu basit şifreleme yönteminde rastgele üretilen bir karakter (harf veya rakam) dizisi kullanılarak şifreleme yapılır.
- Açık mesaj içinde yer alan her karakter, üretilen dizide karşısına denk gelen karakterle işleme sokularak (Örneğin modüler toplama işlemi ile) şifreli mesaj elde edilir. Mesajı çözmek için rastgele dizinin bilinmesi gereklidir. Bu yönteme **Vernam** şifreleme yöntemi denir.
- Açık Mesaj : BULUSMAYERIANKARA
- Rastgele Dizi : DEFRYPLCNMLJKHFGH
- Şifreli Mesaj : RLDYDOY....

Tek Kullanımlı Şifreler

Tek kullanımlı şifreler, geliştiricisi G. Vernam'e dayandırılarak, Vernam Şifresi olarak adlandırılmaktadır.

C=(P+K) mod(29) işlemi Vernam şifresini tanımlar.

Deşifre: (Şifreli karakter – rastgele sayı) mod(29) + 29 = (1-16) +29 = 14 (K)

= (16-78)mod(29) +29 =-4 + 29 = 25(U)

Açık Metin	K	U	S	U	R	S	U	Z	Ş	İ	F	R	E
Sayısal metin	14	25	22	25	21	22	25	29	23	12	17	21	6
Rasgele Sayılar	16	78	130	13	28	16	300	95	628	156	412	863	616
Toplam:	30	103	152	38	49	38	325	124	651	168	429	884	622
Mod(29)	1	16	7	9	20	9	6	8	13	23	23	14	13
Şifreli Metin	A	M	F	Ğ	P	Ğ	E	G	J	Ş	Ş	K	J

Tek Kullanımlık Karakter Dizisi (One-time Pad)

- Bu yöntemin güvenliği rastgele üretilen diziye bağlıdır. Bu dizi gerçekten rastgele üretilmelidir, eğer bir kurala bağlı olarak üretilirse ve bu kural saldırgan tarafından bilinirse sistem kırılabilir. Bu tehdit dışında sistem mükemmel bir şifreleme sistemidir ve ilk olarak 1917'de bulunup "teletype" makinelerinde kullanılmıştır.

Tek Kullanımlık Karakter Dizisi (One-time Pad)

- One-time pad algoritması ile şifreleme yapan örnek bir teletype cihazı.

Günümüzde Kullanılan Simetrik Şifreler

- Blok Kriptolama
  - Veri Kriptolama Standardı (DES)

Simetrik Şifreleme Algoritmaları

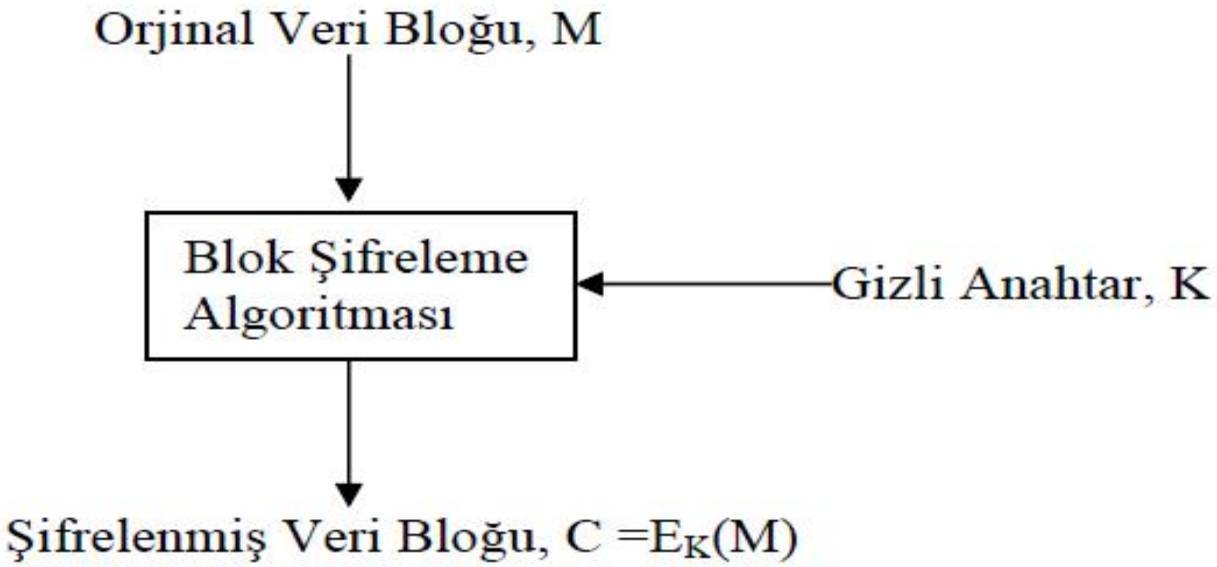
- Simetrik algoritmalar blok şifreleme ve dizi şifreleme algoritmaları olarak ikiye ayrılmaktadır.
- Blok Şifreleme Algoritmaları veriyi bloklar halinde işlemektedir.
- Bazen bağımsız bazen birbirine bağlı olarak şifrelemektedir.
- Bu algoritmalarda iç hafıza yoktur, bu yüzden hafızasız şifreleme adını da almıştır.
- Bütünlük kontrolü gerektiren uygulamalarda genellikle blok şifreleme algoritmaları tercih edilir.

Blok şifreler

Blok sifreleme algoritmaları, orijinal veri olarak bit gruplarını alır. Bu bit gruplarına blok adı verilirken, kullanılan algoritmalara da blok sifreleri (blok ciphers) denir.

Modern bilgisayar algoritmalarında genel olarak tipik blok boyutu, üzerinde analiz yapılmasını engellemeyecek kadar büyük ve çalısma yapılabilecek kadar küçük olmasını sağlamak amacı ile genel olarak 32, 64 veya 128 bit olarak seçilmistir.

Bununla birlikte sözlük ataklarını önleyebilmek amacı ile blok boyunun 64 bit ve üzerinde seçilmesi önerilmektedir .



Simetrik Şifreleme Algoritmaları – Blok Şifreleme Algoritmaları

- Blok şifrelerin gücünü belirleyen bazı faktörler aşağıdaki gibidir:
  - **Anahtar:** Blok şifrelerde anahtarın uzunluğu saldırılara karşı güçlü olacak şekilde seçilmelidir. Anahtarın uzun olması şifrenin kaba kuvvet (brute-force) saldırısına karşı kırılabilirliğini zorlaştırır.
  - **Döngü sayısı:** Blok şifreleme algoritmalarında döngü sayısı iyi seçilmelidir. Böylelikle doğrusal dönüşüm ve yerdeğiştirme işlemleri ile şifreleme algoritması daha da güçlenmektedir. Ayrıca şifrenin karmaşıklığının arttırılmasında çok önemli bir etkendir. Böylelikle saldırılara karşı açık metin iyi derecede korunabilir.
  - **S-kutuları (Yerdeğiştirme kutuları):** Blok şifreleme algoritmalarının en önemli elemanı S-kutularıdır. Algoritmanın tek doğrusal olmayan elemanıdır. Bu yüzden iyi bir S-kutusu seçimi şifrenin karmaşıklığını doğrudan etkiler.

Simetrik Şifreleme Algoritmaları

- Dizi şifreleme algoritmaları ise veriyi bir bit dizisi olarak almaktadır.
- Bir üreteç aracılığı ve anahtar yardımıyla istenilen uzunlukta kayan anahtar adı verilen bir dizi üretilir.
- Kayan anahtar üretimi zamana bağlıdır ve bu yüzden bu algoritmalara aynı zamanda hafızalı şifreleme denir.
- Telsiz haberleşmesi gibi gürültülü ortamlarda ses iletimini sağlamak için genellikle dizi şifreleme algoritmaları kullanılır.

Simetrik Şifreleme Algoritmaları - DES

- DES (Data Encryption Standard) : DES yapısı itibari ile blok şifreleme örneğidir.
- Yani basitçe şifrelenecek olan açık metni parçalara bölerek (blok) her parçayı birbirinden bağımsız olarak şifreler ve şifrelenmiş metni açmak içinde aynı işlemi bloklar üzerinde yapar.
- Bu blokların uzunluğu 64 bittir.

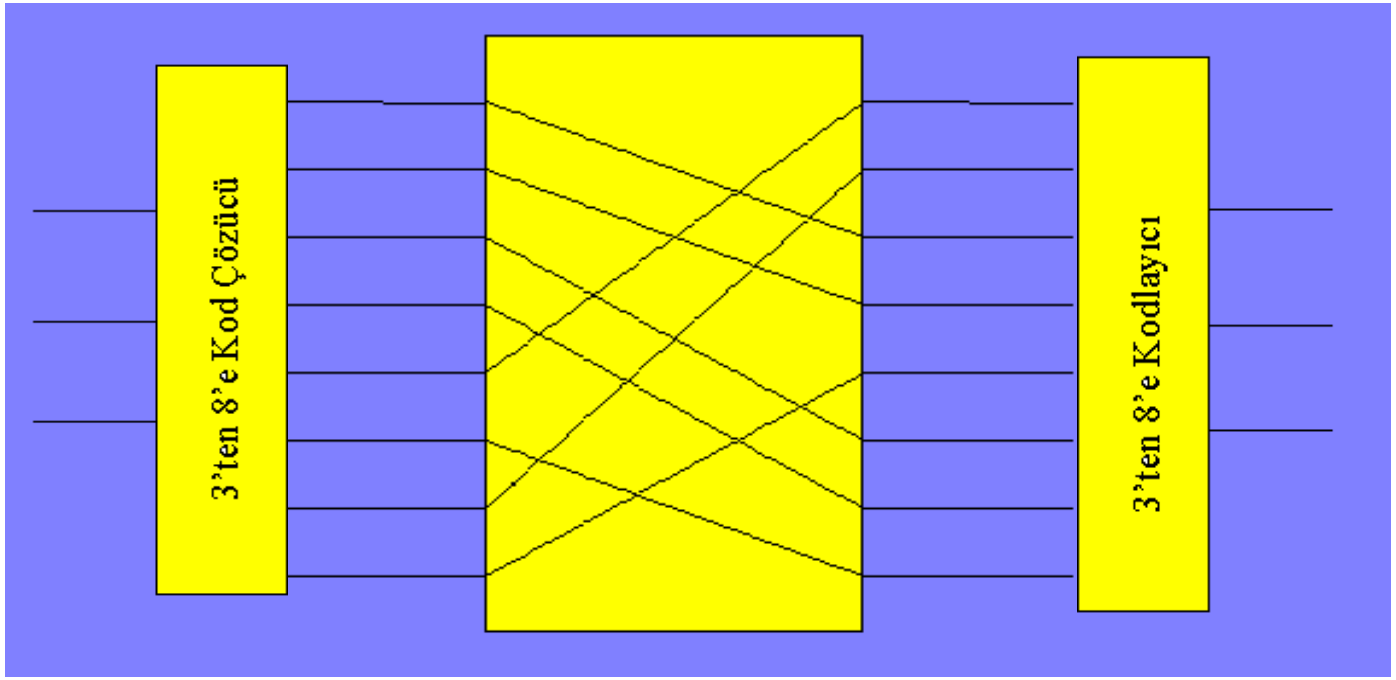
Simetrik Şifreleme Algoritmaları - DES

•DES 64-bit blok üzerinde açık metinleri işler. DES 64 bitlik veri blogunu alır ve baslangıç permütasyonu (initial permütasyon) isleminden sonra 32 bitlik sag ve sol yarılara ayırır.

• Sonra verinin anahtar ve f fonksiyonu ile birlestirildigi 16 döngülük islemler gerçeklestirilir. 16. döngüden sonra sag ve sol yarı tekrar biraraya getirilir.

•Baslangıç permütasyon isleminin tersi olan son permütasyon diger bir deyisle ters permütasyon islemi gerçeklestirilir .

Blok Kriptolama



Permütasyon Kutusu

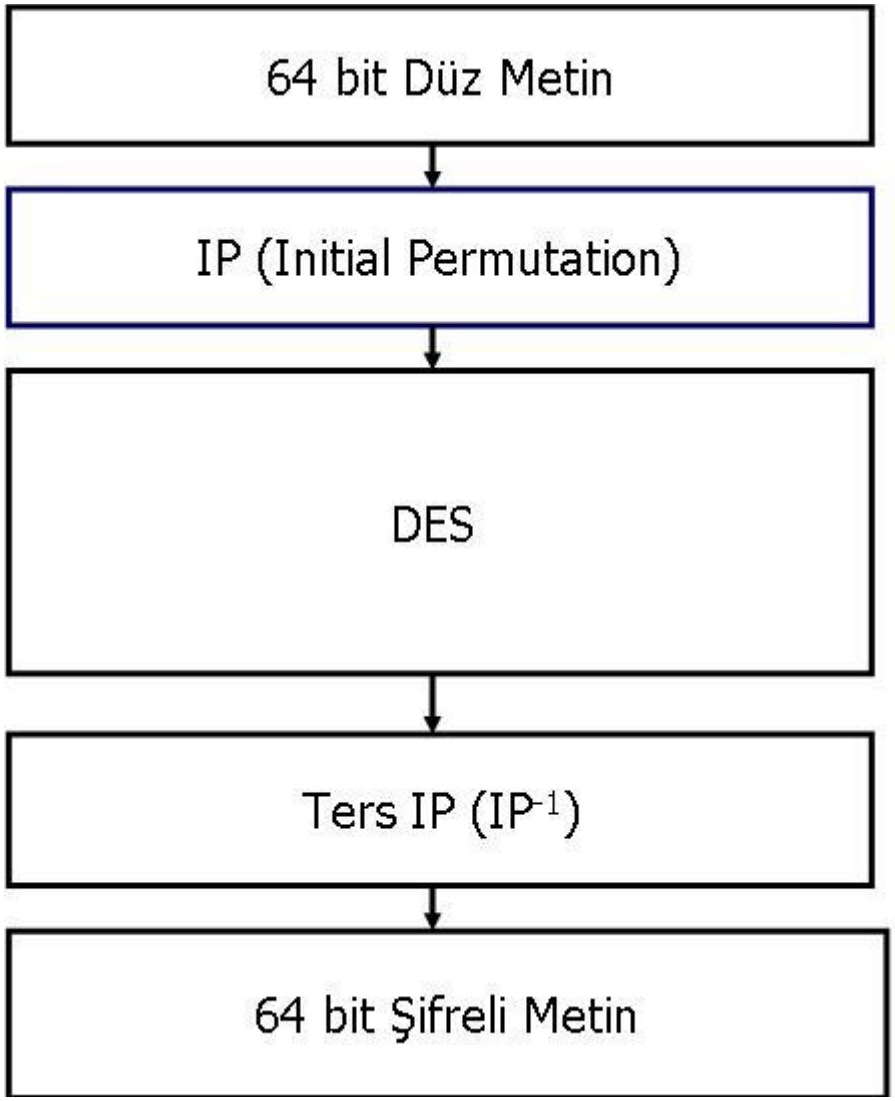
Simetrik Şifreleme Algoritmaları - DES

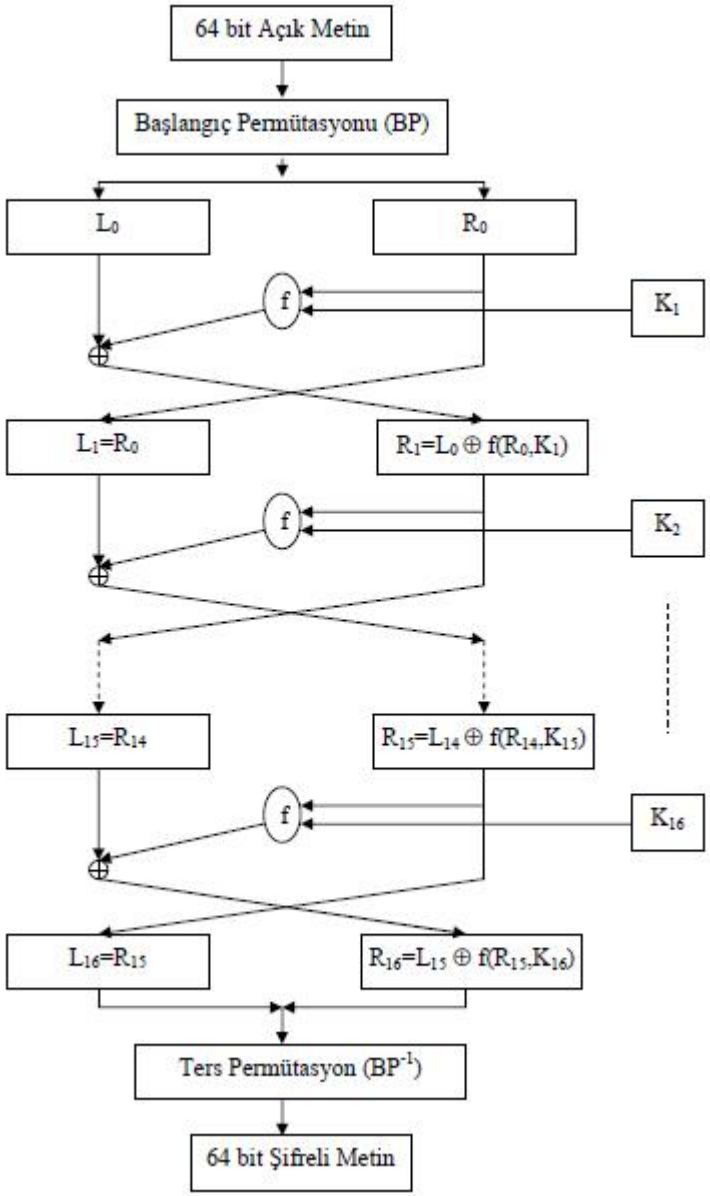
- Dünyada en yaygın kullanılan şifreleme algoritmalarından birisidir.
- DES, IBM tarafından geliştirilmiştir. 1975 yılında “Federal Register” tarafından yayınlanmıştır.
- DES 64 bitlik veriyi 56 bitlik anahtar kullanarak şifreler.
- Kullanılan teknikler yayılma ve karıştırmadır.

Simetrik Şifreleme Algoritmaları - DES

- DES'in en büyük dezavantajı anahtar uzunluğunun 56 bit olmasıdır.
- 1975 yılında yayınlanan bu algoritma günümüzde geliştirilen modern bilgisayarlar tarafından yapılan saldırılar (BruteForce) karşısında yetersiz kalmaktadır.
- Daha güvenli şifreleme ihtiyacından dolayı DES, Triple-DES olarak geliştirilmiştir.
  - Triple -DES algoritması geriye uyumluluğu da desteklemek amacıyla 2 adet 56 bitlik anahtar kullanır.

DES Algoritması Genel Yapısı.




64 bit Açık Metin
Başlangıç Permütasyonu (BP)
L0
R0
f
K1
L1=R0
R1=L0 ⊕ f(R0,K1)
f
K2
L15=R14
R15=L14 ⊕ f(R14,K15)
f
K16
L16=R15
R16=L15 ⊕ f(R15,K16)
Ters Permütasyon (BP-1)
64 bit Şifreli Metin

Başlangıç Permütasyonu

Tablo 7.1. Başlangıç Permütasyonu (BP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Bir DES döngüsünde gerçeklestirilen islemler

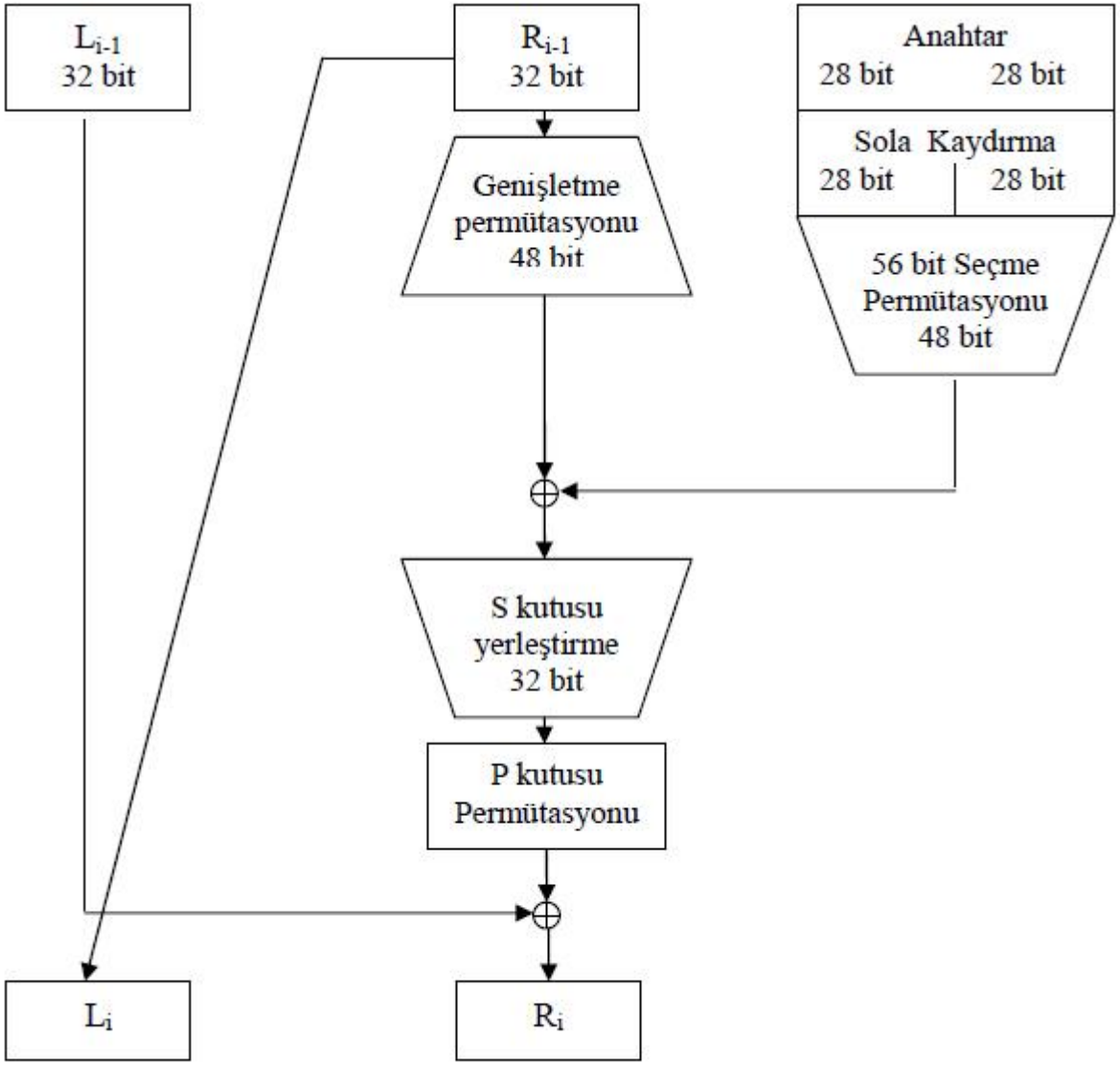
Her döngüde anahtar (sifreleme ise sola, çözme ise saga) kaydırılır ve 56 bitin 48'i seçilir. Sag yarıdan gelen 32 bit, genislemis permütasyon yardımı ile 48 bite dönüstürülür ve 48 bitlik anahtar ile XOR'lanır.

Sonuç 8 tane S-kutusuna gönderilir. Çıkısta 32 bit üretilir ve çıkıs bitlerine P permütasyonu uygulanır. Bu dört islem f fonksiyonunu olusturur.
f fonksiyonunun çıkısı soldan gelen 32 bitlik veri ile XOR'lanır. Bu islemin sonucu yeni sag yarıyı, eski sag yarı da yeni sol yarıyı olusturur. Bu islemler 16 kez tekrarlanarak DES'in 16 döngüsü gerçeklestirilmis olur.

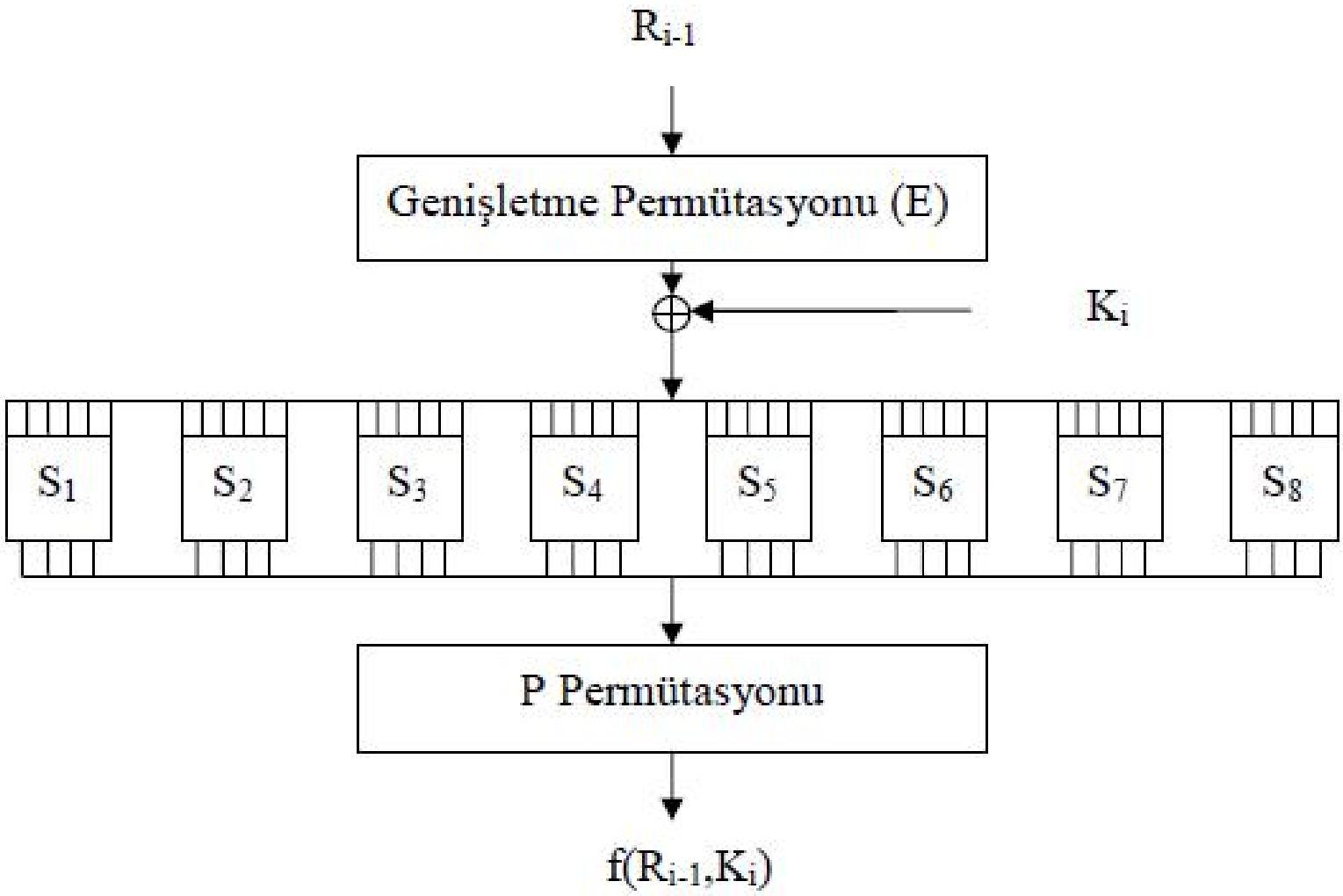
Her bir döngüdeki işlemler aşağıdaki gibidir.

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$



Sekil 7.2. Bir DES Döngüsünde Gerceklestirilen İslemler


R_{i-1}
Genişletme Permütasyonu (E)
K_i
S_1
S_2
S_3
S_4
S_5
S_6
S_7
S_8
P Permütasyonu
$f(R_{i-1},K_i)$

Ters permütasyon

Yukarıda anlatılan islemler 16 kez gerçeklestirildikten sonra baslangıç permütasyonu isleminin tersi olan ters (son) permütasyonu asagıda verilen sekile göre gerçeklestirilir.

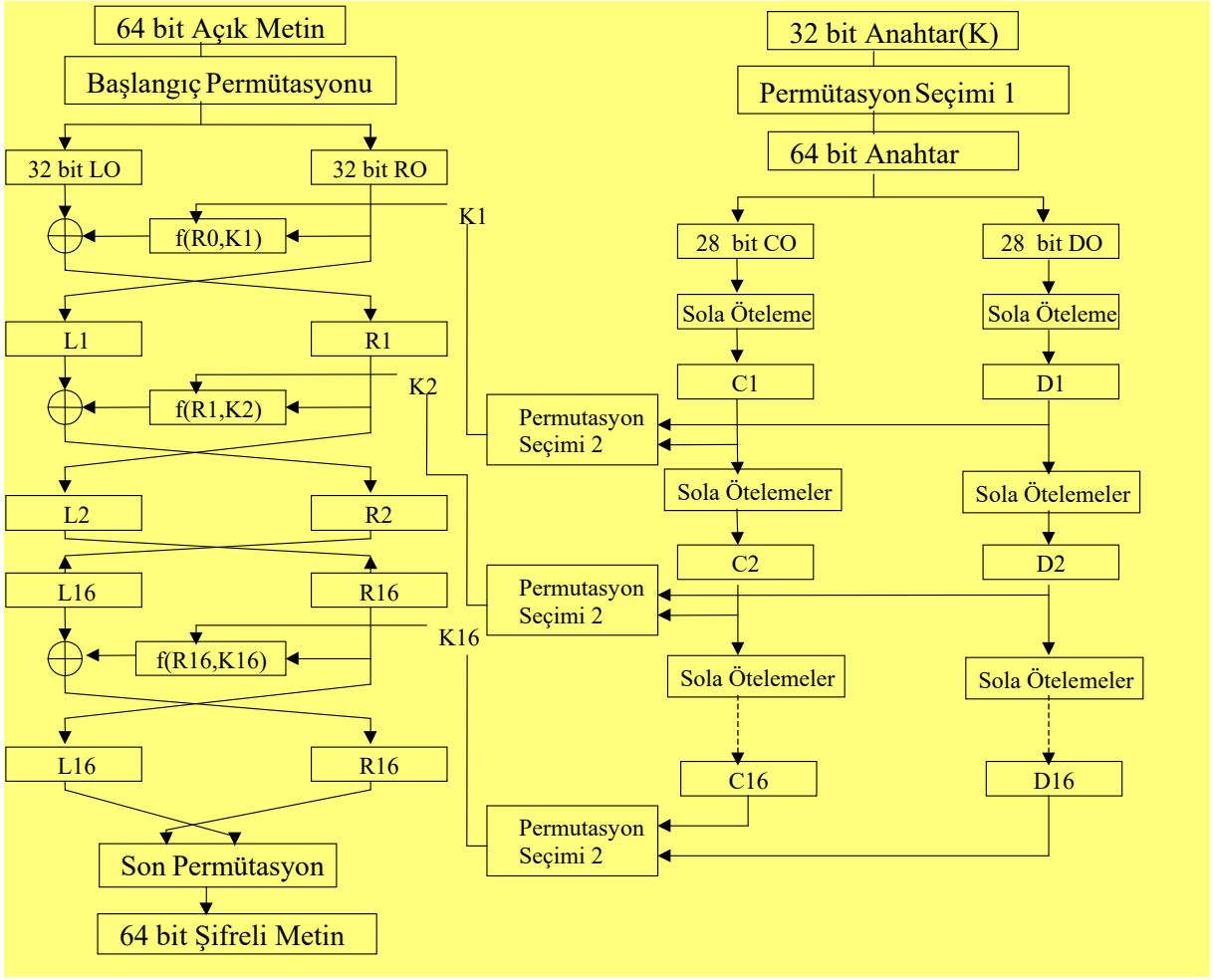
Bu tabloya göre 40. bit 1. bit, 8. bit 2. bit vb. olarak çıkar.

Tablo 7.5. Ters Permütasyon (BP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Veri Şifreleme Standardı (DES)

Algoritma 56 biti asıl anahtar, geri kalan 8'i parite biti olarak kullanılmak üzere seçilmiş 64 bitlik anahtar kullanır. Açık metin 64 bitlik bloklar halinde kriptolanır ve 64 bitlik gizli metin çıktısı elde edilir.



Simetrik Şifreleme Algoritmaları – Triple DES

- Triple-DES, IBM tarafından geliştirilip 1977'de standart olarak kabul edilmiştir.
- Fakat 1997 yılında İsrail'liler tarafından kırılmış bulunmaktadır.
- Şifreleme metodunun çözülmüş olmasına rağmen günümüz bankacılık sistemlerinde kullanılmakta olan şifreleme sistemidir.
- Triple-DES algoritması, DES algoritmasının şifreleme, deşifreleme, şifreleme şeklinde uygulanmasıdır.

Simetrik Şifreleme Algoritmaları – Triple DES

- Standart DES'in 112 veya 168 bitlik iki veya üç anahtar ile artarda çalıştırılması ile oluşturulan bir şifreleme tekniğidir.
- Anahtar alanı 2112 veya 2168 sayısına ulaşınca bugün için veya tahmin edilebilir bir gelecekte çözülmesi mümkün olmayan bir kod olmaktadır

Simetrik Şifreleme Algoritmaları – Twofish

- 1993 yılında yayınlanan bu algoritma Bruce Schneier - John Kelsey - Doug Whiting – David Wagner - Chris Hall - Niels Ferguson tarafından oluşturulmuş simetrik blok şifreleme algoritmasıdır.
- AES kadar hızlıdır.
- Aynı DES gibi Feistel yapısını kullanır.
- DES'den farklarından biri anahtar kullanılarak oluşturulan değişken S-box (Substitution box – Değiştirme kutuları)' lara sahip olmasıdır.

Simetrik Şifreleme Algoritmaları – Twofish

- Ayrıca 128 bitlik düz metni 32 bitlik parçalara ayırarak işlemlerin çoğunu 32 bitlik değerler üzerinde gerçekleştirir.
- AES'den farklı olarak eklenen 2 adet 1 bitlik rotasyon, şifreleme ve deşifreleme algoritmalarını birbirinden farklı yapmış, bu ise uygulama maliyetini arttırmış, aynı zamanda yazılım uygulamalarını %5 yavaşlatmıştır

Simetrik Şifreleme Algoritmaları – IRON

- Diğer iki algoritma gibi Feistel yapısını kullanır.
- IRON, **64 bitlik veri bloklarını 128 bitlik anahtarla** şifrelemede kullanılır.
- Döngü (round) sayısı 16 ile 32 arasındadır.
- Alt anahtarların sayısı döngü sayısına eşittir.
  - Bu nedenden dolayı **algoritma anahtar bağımlıdır.** Var olan algoritmalardan **farkı da** budur.
- Bu algoritmanın avantajı **bitler yerine 16-tabanındaki (hex) sayılar kullanmasıdır, dezavantajı** ise **yazılım için tasarlanmış olmasıdır.**

Simetrik Şifreleme Algoritmaları – AES

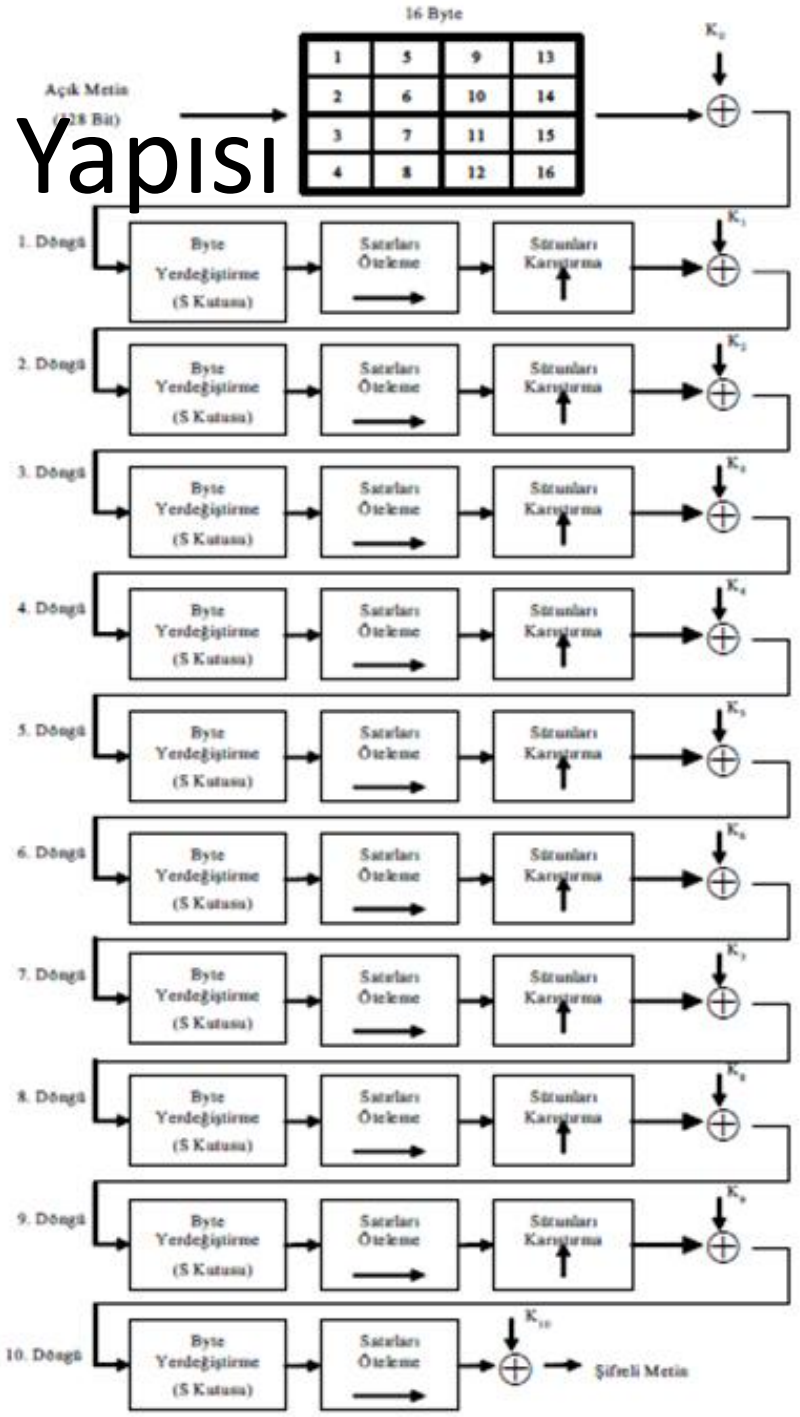
- AES, John Daemen ve Vincent Rijmen tarafından **Rijndael adıyla geliştirilmiş ve 2002 yılında standart** haline gelmiştir.
- AES uzunluğu **128 bitte sabit olan blok** ile uzunluğu **128, 192 ya da 256 bit olan anahtar** kullanır.
- Kullanılan tekniklerden bazıları baytların yer değiştirmesi, **4x4' lük matrisler üzerine yayılmış metin** parçalarının satırlarına uygulanan kaydırma işlemleridir.
- **2010 yılı itibariyle en popüler simetrik algoritmalardan biridir.**

Simetrik Şifreleme Algoritmaları – IDEA

- IDEA (International Data Encryption Algorithm) 1991 yılında geliştirilmiştir.
- 128 bit anahtar uzunluğu kullanır.
- XOR, 16 bit tam sayı toplama ve 16 bit tam sayı çarpma matematik işlemlerini kullanır.
- Alt anahtar üretim algoritması dairesel kaydırma üzerinedir.

AES Döngü Yapısı

	Kelime Uzunluğu	Tur Sayısı
AES-128	4	10
AES-192	6	12
AES-256	8	14



AES Döngü Yapısı

- Her döngü tersi alınabilir dönüşümler kullanır.
- Her döngü, son döngü hariç, 4 dönüşüm kullanır: SubBytes, ShiftRows, MixColumns ve AddRoundKey.
- Son döngüde MixColumns dönüşümü göz ardı edilir.
- Her döngüde farklı anahtar materyali kullanılır.
- Farklı anahtar materyalleri anahtar planlama evresinde gelen anahtarlardır. Master anahtardan farklı anahtarlar elde edilerek şifrede kullanılır.
- Deşifreleme kısmında ters dönüşümler kullanılır: InvSubByte, InvShiftRows, InvMixColumns ve AddRounKey (tersi kendisidir- XOR işlemi).

Simetrik Şifreleme Algoritmaları – 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.

Simetrik Şifreleme Algoritmaları – MD5

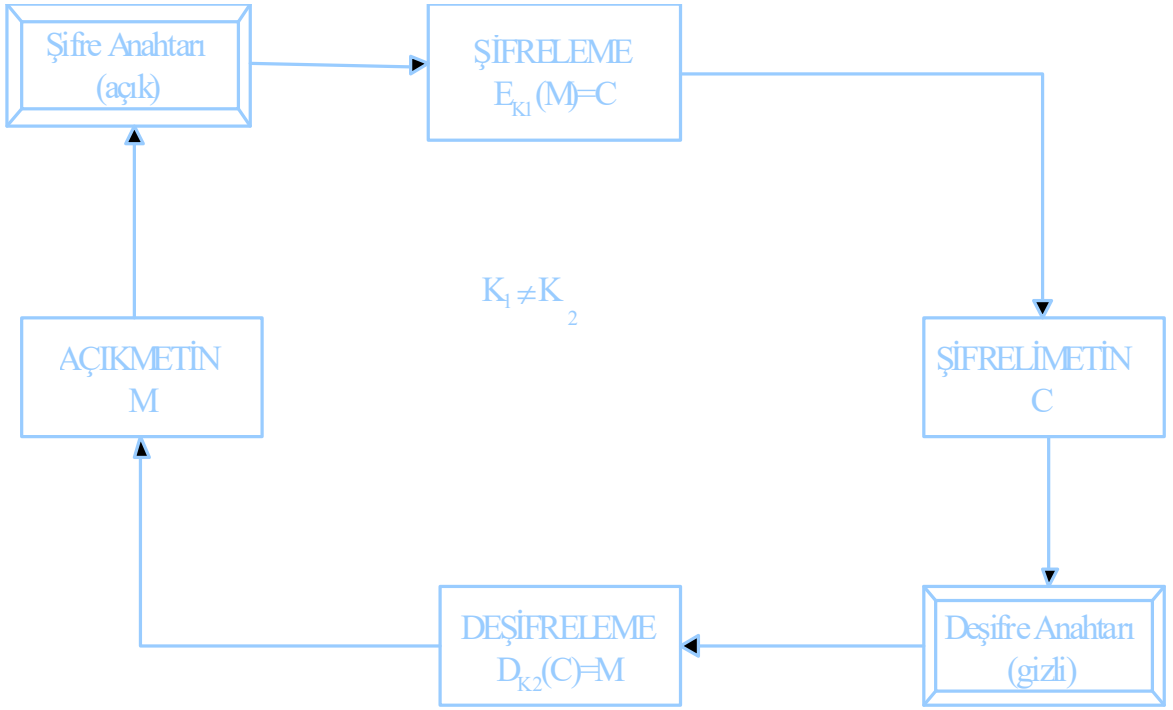
- MD5 (Message-Digest algorithm 5) Ron Rivest tarafından 1991 yılında geliştirilmiş bir tek yönlü şifreleme algoritmasıdır
- Veri bütünlüğünü test etmek için kullanılan, bir şifreleme algoritmasıdır.
- Bu algoritma girdinin büyüklüğünden bağımsız olarak 128-bit'lik bir çıktı üretir ve girdideki en ufak bir bit değişikliği bile çıktının tamamen değişmesine sebep olur.
- MD5'ın en çok kullanıldığı yerlerden biri, bir verinin (dosyanın) doğru transfer edilip edilmediği veya değiştirilip değiştirilmediğinin kontrol edilmesidir.

Simetrik Şifreleme Algoritmaları – SHA

- SHA (Secure Hash Algorithm – Güvenli Özetleme Algoritması), Amerika'nın ulusal güvenlik kurumu olan NSA tarafından tasarlanmıştır.
- SHA-1, uzunluğu en fazla 264 bit olan mesajları girdi olarak kullanır ve 160 bitlik mesaj özeti üretir.
- Bu işlem sırasında, ilk önce mesajı 512 bitlik bloklara ayırır ve gerekirse son bloğun uzunluğunu 512 bite tamamlar.
- SHA-1 çalışma prensibi olarak R. Rivest tarafından tasarlanan MD5 özet fonksiyonuna benzer.
- 160 bitlik mesaj özeti üreten SHA-1 çakışmalara karşı 80 bitlik güvenlik sağlar.

Asimetrik Kripto Sistemler

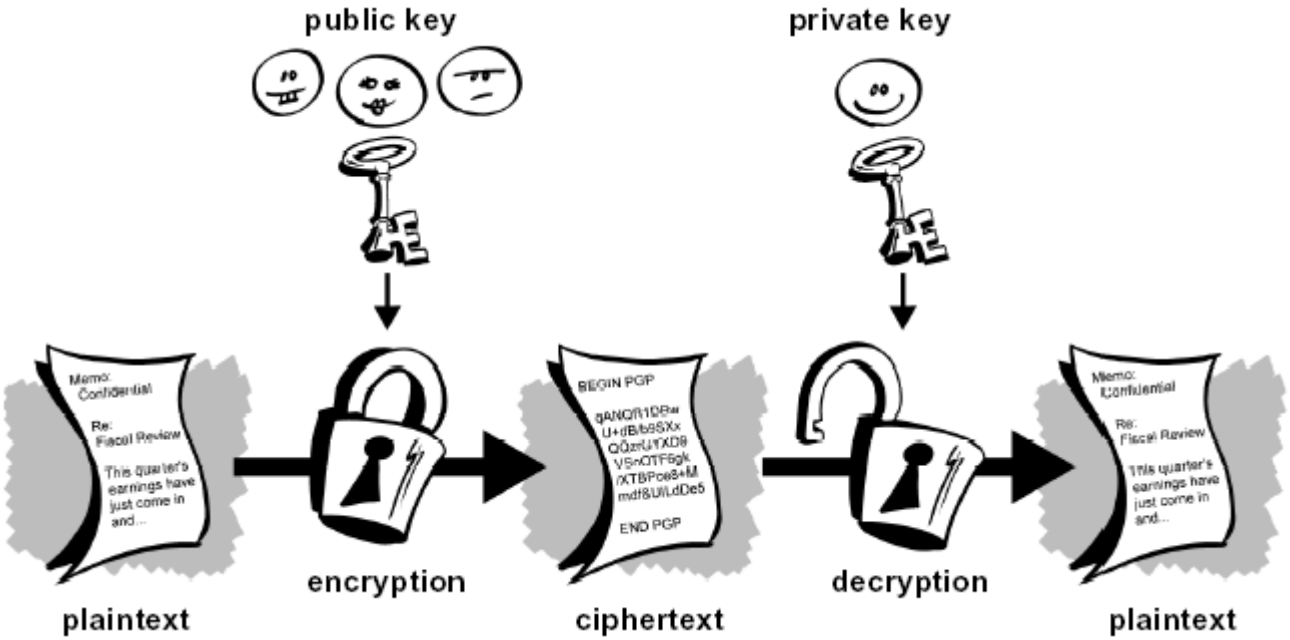
- Rivest-Shamir-Adleman (RSA) Kripto Sistemi
- El Gamal Kripto Sistemi



Asimetrik Şifreleme Algoritmaları

- 1976 yılında Stanford Universitesinden Diffie ve Hellman adlı araştırmacılar iki farklı anahtara dayalı şifreleme sistemi önermiştir.
- Bu sistemde bir tane şifreleme için (public key) ve bundan farklı olarak bir tanede şifre çözmek için(private key) anahtar bulunur.
- private key, public key' den elde edilemez.
- Asimetrik şifreleme algoritmalarında çok büyük asal sayılar kullanılmaktadır.

Asimetrik Şifreleme Algoritmaları



Asimetrik Şifreleme Algoritmaları

- Kuvvetli Yönleri;
  - Kriptografinin ana ilkeleri olarak sayılan; bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir.
  - Anahtarı kullanıcı belirleyebilir.
- Zayıf Yönleri;
  - Şifrelerin uzunluğundan kaynaklanan algoritmaların yavaş çalışması.
  - Anahtar uzunlukları bazen sorun çıkarabiliyor olması.

Asimetrik Şifreleme Algoritmalarının Avantajları

- Asimetrik şifrelemenin kırılması simetrik şifrelemeye göre daha zordur.
- Bu yöntem private-key' lerin karşılıklı aktarılmasını gerektirmez.
  - Böylece simetrik şifrelemedeki anahtar dağıtım problemi çözülmüş olur.
- Public Keylerin bize şifreli mesaj göndermek isteyenler tarafından bilinmesi gerektiğinden bu anahtarlar internette bir sunucu ile rahatça dağıtılmaktadır.
- İki anahtarla şifrelemeden dolayı inkar edememeyi sağlayan sayısal imza gibi yeni yöntemler geliştirilmiştir.

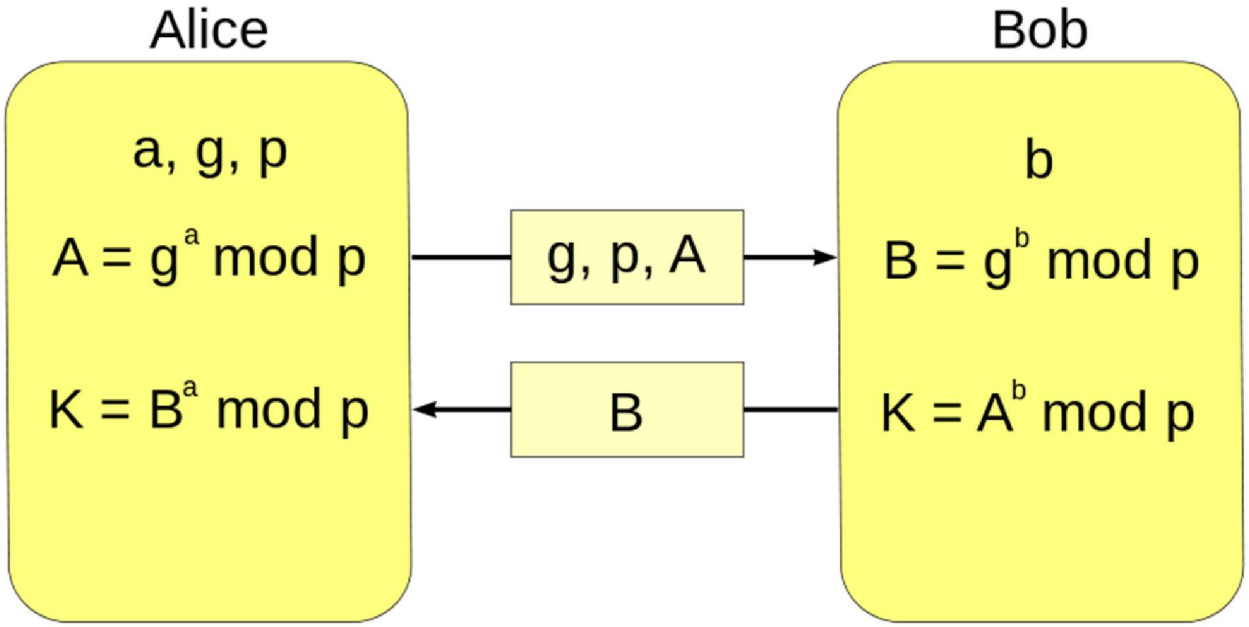
Asimetrik Şifreleme Algoritmalarının Dezavantajları

- Anahtarları kullanarak bilgileri çözme işlemlerinde CPU zamanının çok fazla olması.
- Bu zaman ileti uzunluğu ile üssel olarak artmaktadır.

Asimetrik Şifreleme- Diffie Helman Algoritması

- 1976 yılında Diffie ve Helman tarafından bulunmuş ilk asimetrik şifreleme algoritmasıdır.
- DH iki katılımcının öncesinde herhangi bir bilgi alışverişi yapmadan güvenli olmayan bir kanal vasıtasıyla (güvenli bir şekilde) ortak bir şifrede karar kılmalarına yarayan bir protokoldür.
- Algoritma anahtar değişimi ile asıl amacı, iki kullanıcının bir anahtarı güvenli bir şekilde birbirlerine iletmeleri ve daha sonrasında da bu anahtar yardımı ile şifreli mesajları birbirlerine gönderebilmelerini sağlamaktır.
- Diffie–Hellman algoritması oluşturularak simetrik şifreleme algoritmaları için büyük problemi olan gizli anahtarı koruma ve dağıtım büyük ölçüde aşılmıştır.
- Bununla birlikte Diffie-hellman algoritması sadece ortak gizli anahtarı belirlemekte kullanılmaktadır.

Dikkat Önemli: p sayısının asal sayı seçilmesinin önemi. Asal sayıların ayrık logaritmasının (dscrete lsonucunun bulunması oldukça zordur. Çünkü asal olmayan herhangi bir **p** sayısı için, p sayısını asal çarpanlarına ayırıp, ardından Çin Kalan Teoremi'ni kullanarak problemi kolayca çözebiliriz. Ondan dolayı ilk şart, p sayısının asal sayı olarak seçilmesidir. Dahası problemin çözülebilirliğini zorlaştırmak (şifrenin kırılmasına denk gelir) için asal sayının büyük bir asal sayı olması gerekir.**Araştır .....**



a: Alice'in özel anahtarı, b: Bob'un özel anahtarı
G(Generator) : seçilmiş (iki taraf için), p (prime-asal sayı): Seçilmiş (iki taraf için)
K: Hesaplanan gizli anahtar (Her iki taraf için)

DIFFİE-HELMAN algoritması basit

- **Örnek:**

- Anahtar değişimi yapacak iki tarafta **p=23** ve **g=5** sayılarını kararlaştırıyorlar (bu sayılar iki taraftan da biliniyor ve genel şifreler).
- Ali özel anahtarı olarak **a=6**, seçer ve Barış'a gönderir **(g^a mod p)**

  5^6 mod 23 = 8
- Barış özel anahtarı olarak **b=15** seçer ve Ali'ye gönderir **(g^b mod p)**

  5^{15} mod 23 = 19
- Ali **(g^b mod p)** mod p denklemini hesaplar…….. **19^6 mod 23 = 2**
- Barış **(g^a mod p)** mod p denklemini hesaplar …… **8^{15} mod 23 = 2**

- Sonuçta gidip gelen bilgi 8 ve 19 olmaktadır. Ayrıca herkes tarafından umumî şifrelerde bilinmektedir. Ancak 2 anahtar değerini sadece Ali ve Barış bilebilmektedir. Bu da ancak şifreyi ilgili formülden geçirdikten sonra mümkün olmaktadır.

Asimetrik Şifreleme Algoritmaları - RSA

- Dünyada en yaygın biçimde kullanılan asimetrik algoritma, ismini mucitlerinin baş harflerinden (Ronald L.Rivest, Adi Shamir ve Leonard Adleman) almıştır.
- Büyük sayıların moduler aritmetiğine dayalı çok basit bir prensibi vardır.
- Anahtarlar, iki büyük asal sayıdan üretilir.
- Dolayısıyla, algoritmanın güvenliği büyük sayı üretme problemine dayalıdır

Asimetrik Şifreleme Algoritmaları - RSA

- Örnek:
  - P=7 ve Q=17 gibi iki asal sayı seçilsin.
  - Bu iki asal sayının çarpımı N = P.Q=7*17;**N=119** ve bu sayıların bir eksiklerinin çarpımı ϕ(N)=(P-1)(Q-1)=6*16; **ϕ(N)=96** olarak hesaplanır.
  - 1'den büyük ϕ(N)**(96)**'den küçük aralalığında asal bir **E=5** tamsayısı seçilsin.
  - Seçilen E=5 tamsayısının mod 96'da tersi alınır, sonuç **D=77**'dir.
  - mod(96)=1 eşitliğini sağlayan 0-96 arasındaki E*D çarpımındaki D değerinin bulunuşu. (E*D mod(96) =1 sağlayan D değeri)
  - **E=5** ve **N=119** tamsayıları genel anahtarı, **D=77** ve **N=119** tamsayıları ise özel anahtarı oluşturur.

- (5,119) anahtarları ile şifreleme, (77,119) anahtarı ile deşifreleme yapılacaktır. M açık metni 19 olarak seçilsin.

  - $C=M^E \pmod N \rightarrow C=19^5 \pmod{119} \rightarrow C=66$
  - $M= C^D \pmod N \rightarrow M= 66^{77} \pmod{119} \rightarrow M=19$

Asimetrik Şifreleme Algoritmaları - DSA

- DSA (Digital Signature Algorithm) , NIST tarafından sayısal imza standardı olarak yayınlanmıştır.
- Amerika Birleşik Devletleri tarafından kullanılan dijital doğrulama standartlarının bir parçasıdır.
- DSA “discrete logarithm” problemine dayanır ve Schnorr ve ElGamar tarafından geliştirilen algoritmalarla benzer yapıdadır.
- RSA’dan farkı sadece imzalama amaçlı kullanılabilmesi, şifreleme yapılamamasıdır.

Asimetrik Şifreleme Algoritmaları – Eliptik Eğri Algoritması (ECC)

- ECC şifreleme algoritmasının en büyük özelliği diğer açık anahtar şifreleme sitemlerinin güvenliğini daha düşük anahtar değerleriyle sağlayabilmesidir.
- 1024-bitlik anahtar kullanan RSA şifreleme algoritmasının sağladığı güvenlik gücünü, 160-bit anahtar kullanan ECC sağlayabilmektedir.
- Bu açık anahtarlı algoritmalar içinde çok önemli bir avantajdır.
- Yeni gelişen teknolojiyle birlikte kablosuz ağların kullanımı geniş anahtar değerlerine sahip şifreleme algoritmalarının kullanımını zorlaştırmıştır.
- ECC daha düşük anahtar değerlerini kullanması ve aynı güvenlik seviyesini sağlaması sayesinde kablosuz ağlarda kullanımına çok uygundur.