Kriptografik Sistemler

CCNA Security

Cisco | Networking Academy®
Mind Wide Open™

Bölüm 7

7.1 Kriptografik servisler

7.2 Basitlik Bütünlük ve Kimlik Doğrulama

7.3 Gizlilik

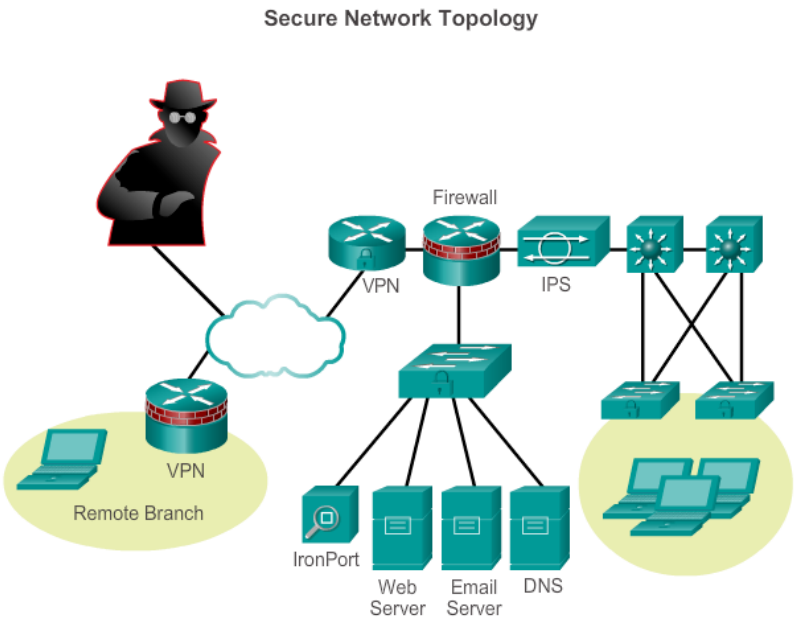
7.4 Genel Anahtar Kriptografisi

7.1 Kriptografik Servisler

Cisco Networking Academy®
Mind Wide Open™

Kimlik Doğrulama, Bütünlük ve Gizlilik

- Güvenli haberleşmeyi sağlamak için network yöneticilerinin birincil amacı router, switch, bilgisayar ve sunucuları içeren network arayüzünü güvenli hale getirmektir.
- Bir LAN aşağıdakilerle güvenli hale getirilebilir:
  - Cihaz güvenliği
  - Erişim kontrolü
  - Firewall özellikleri
  - IPS uygulamaları
- İnternet ortamından geçen trafik nasıl güvenli hale getirilebilir? Kriptoloji metotları kullanılarak.



Kimliklendirme, Bütünlük ve Gizlilik

Güvenli haberleşme şu üç durumu gerektirir:

- **Authentication (Kimlik Doğrulama) –** Mesajın bir sahtekarlık içermediği ve bir sahtekardan gelmediğinden emin olunmalıdır.
- **Integrity (Bütünlük) –** Mesajın bir başkası tarafından ele geçirilip değiştirilmediğinden emin olunmalıdır. Tıpkı frame checksum'ı gibi.
- **Confidentiality (Gizlilik) –** Mesaj yakalanmış olsa bile anahtarının açılmamış olduğundan emin olunmalıdır.

Authentication


Integrity

Confidentiality

Kimlik Doğrulama

- Kimlik doğrulama mesajın şu özelliklerini garanti eder:
  - Sahtecilik içermez.
  - Doğru kişiden gelmiştir.
- Kimlik doğrulama ATM cihazlarında banka kartı PIN'i gibidir.
  - PIN sadece kullanıcı ve banka tarafından bilinir.
  - PIN, paylaşılmış bir gizliliktir ve sahtecilikten korur.

Entering an ATM Authentication PIN

Güvenli Haberleşme

Kimlik Doğrulama

- Mesajın gönderici tarafından tekil olarak oluşturulmasını sağlar.
- Yani mesaj gönderici tarafından izinli olarak gönderilmiş demektir.

Veri Bütünlüğü

- Veri bütünlüğü verinin transferi esnasında değiştirilmediğini garanti eder. Alıcı gelen mesajın göndericiden çıktığı haliyle alındığını doğrulayabilir.
- Eskiden mektupların açılmadığını garanti etmek için zarfın ağzı balmumu mühür ile yapıştırılırdı.
  - Mühür çoğu zaman mühür yüzüğü ile yapılırdı.
  - Kırılmamış bir mühür onun içeriğinin bozulmadığını gösterir.
  - Aynı zamanda tekil mühür yüzüğü kimlik doğrulamayı sağlar.

An Unbroken Wax Seal Ensures Integrity

Güvenli Haberleşme

Veri Bütünlüğü

- Veri bütünlüğü mahremiyeti sağlar. Yani sadece alıcı mesajı okuyabilir.
- Kriptolama, verinin yetkisiz biri tarafından okunamayacak şekilde karıştırılmasıdır.
  - Okunabilir veriye plaintext (düz metin) veya cleartext (açık metin) denir.
  - Kriptolanmış veriye ciphertext (şifreli metin).
- Bir mesajı kriptolama veya çözme için bir anahtar gerekir. Anahtar plaintext ve ciphertext arasında bir bağdır.

Ciphertext Oluşturma

- Kimlik doğrulama, bütünlük ve gizlilik kriptografinin bileşenleridir.
- Kriptografi hem bilgi gizleme çalışmaları hem de uygulamalarıdır.
- Yüzyıllardır dökümanları gizlemek için kullanılıyor. Günümüzde modern tekniklerle güvenli haberleşme yapılabilmektedir.

Authentication

Integrity

Confidentiality

Ciphertext Oluşturma

- Kriptolama metotları kodlama ve çözme için özel algoritmalar kullanırlar. Bunlara cipher (parola) denir.
- Bir parola iyi tanımlanmış adımlar serisi içeren bir prosedürdür.
- Şifreli metin oluşturmanın birkaç metodu vardır:
  - Transposition (Aktarma)
  - Substitution (Değiştirme)
  - One-time pad (Bir seferlik şifreleme)

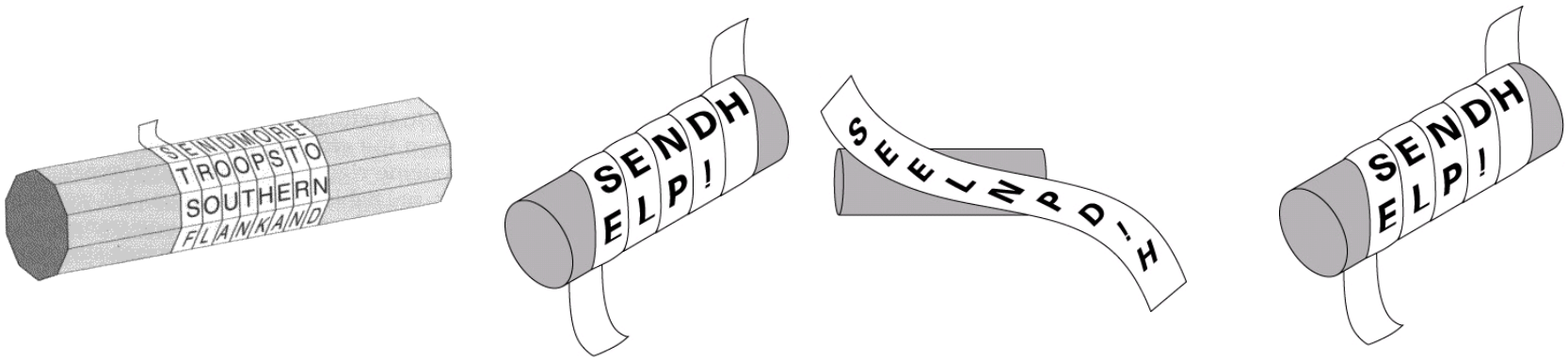
Ciphertext Oluşturma

- Kriptografik servisler bir çok güvenlik uygulamasının temel dayanağıdır.
- Yüzyıllar boyunca çeşitli şifreleme metotları kullanılmıştır:
  - Scytale
  - Caesar cipher
  - Vigenère Cipher
  - Jefferson’s encryption device
  - German Enigma machine

Ciphertext Oluşturma

Scytale

- Eski Yunanda Spartan adlı kral tarafından ilk kriptolama yöntemidir.
- Kodlanacak metin şerit halinde kesilip bir çubuğun etrafına dolanmış kağıt üzerine yazılır. Çözmek için aynı çubuk gereklidir



Ciphertext Oluşturma

Caesar Cipher

- Sezar generallerine mesaj gönderirken elçilere ve ulaklara güvenmediği için şifreleyip gönderirdi.
- Sezar her harfi bir başka harfle değiştirerek gönderir:
  - A ile D
  - B ile E
  - Ve diğerleri
- Generaller üç harf kaydırma kuralını bildikleri için mesajları okuyabiliyorlardı.

Vigenère Cipher

Vigenère Cipher

- 1586'da, Frenchman Blaise de Vigenère kriptolama için çok alfabeli bir sistem tanımladı. Vigenère Cipher olarak anıldı.
- Sezar şifrelemesini esas alır ancak çoklu karakterli anahtar kullanır. Bu aynı zamanda otomatik anahtar şifrelemesi anlamına da gelir.

Kriptografi

Vigenère Cipher

	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
A	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
B	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	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	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
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
F	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	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	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
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
J	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	i
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
L	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	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	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
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
T	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	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	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

Ciphertext Oluşturma

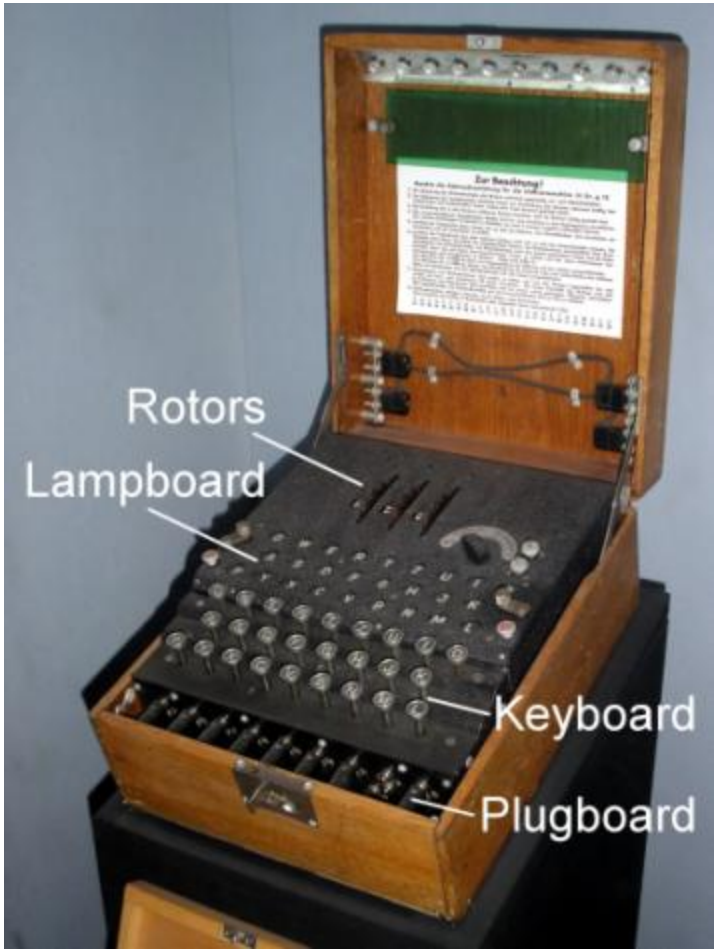
Jefferson Kripto Cihazı

- 3. Amerika Başkanı Thomas Jefferson bir kripto sistemi icat etti. 1790-93 yılları arasında kullanıldı.

Ciphertext Oluşturma

Enigma Makinesi

- Arthur Scherbius 1918'de Enigmayı keşfetti ve Almanya'ya sattı. Bu makine diğer makinelerin şablonu olarak kullanıldı ve II. Dünya Savaşı boyunca kullanıldı.
- 1000 kripto analizcisi tarafından dakikada 4 anahtarla günlerce denense 1,8 milyar yıl alacaktı.
- Almanya Enigma'nın kriptoladığı belgeler düşmanların eline geçse bile çözülemeyeceğini biliyorlardı.



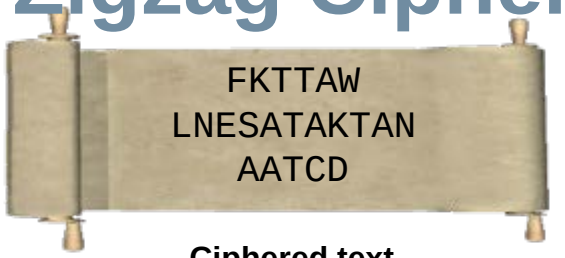
http://users.telenet.be/d.rijmenants/en/enigma.htm

Transposition Ciphers

- Transpozisyon şifrelemede hiçbir harf değiştirilmez, sadece yeniden dizilir.
- Data Encryption Standard (DES) ve 3DES gibi modern kripto algoritmaları hala algoritmanın bir parçası olarak transpozisyonu kullanır.

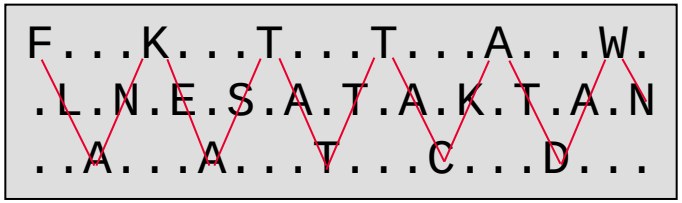
Transposition Ciphers - Zigzag Cipher

1. Ciphertext çözme.

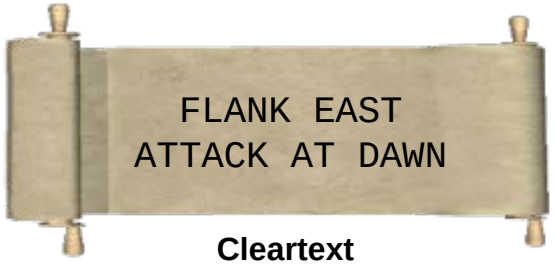


Ciphered text

2. 3 harfli bir zig zag oluşturulur.



3. Cleartext mesaj elde edilir.



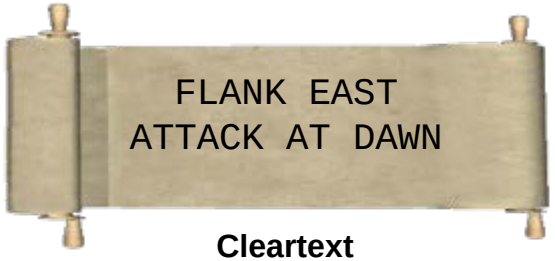
Cleartext

Substitution Ciphers

- Değiştirme şifrelemeleri bir harfi bir başka harfle değiştirir. Basit formunda, harf sıklığı korunur.
- Örnekler:
  - Caesar Cipher
  - Vigenère Cipher

Substitution Ciphers – Sezar Şifresi ile Kodlama

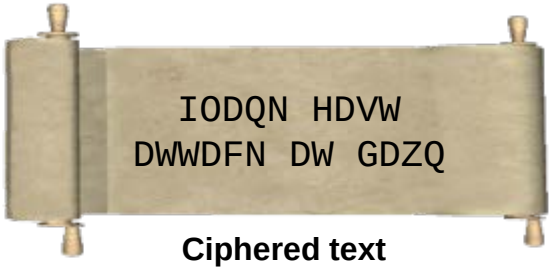
1. Cleartext message.



Cleartext

2. 3 anahtarı ile kodlanır. Bu yüzden, A yerine D, B yerine E, … yazılır

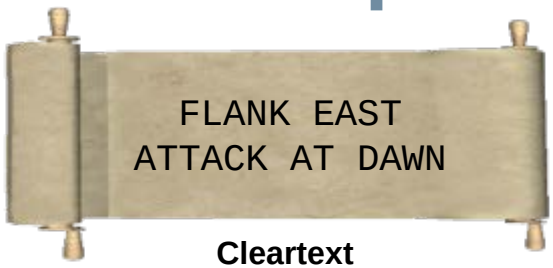
3. Kodlanmış mesaj elde edilir



Ciphered text

Substitution Ciphers - Caesar Cipher Disk

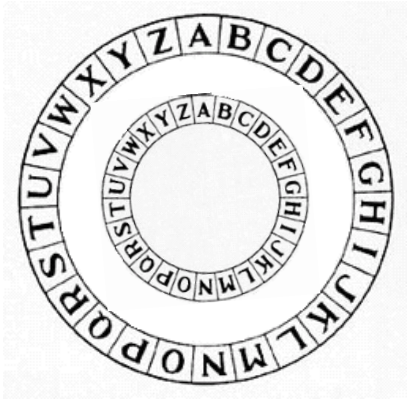
1

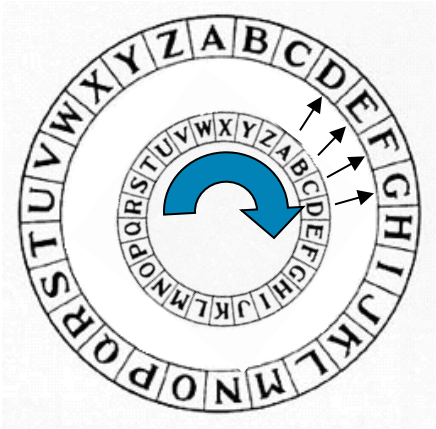


Cleartext

Şifresiz metin 3 anahtarı kullanılarak codlanır.

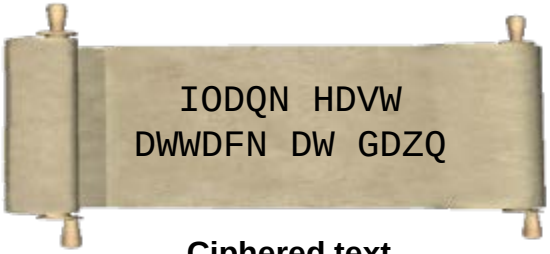
2





İçteki disk 3 diş döndürülür. Böylece kaymalar elde edilir.

3



Ciphered text

Şifreli metin elde edilir.

Substitution Ciphers - Vigenère Cipher

- Vigenère şifresi Sezar şifresini esas alır. Farklı çoklu alfabe kullanması hariç.
  - Farklı alfabe kaydırması gönderici ile alıcı arasında paylaşılmış bir anahtar olarak belirlenir.
  - Şifresiz metin Vigenère şifre tablosu kullanılarak kodlanabilir.
- Örneğin:
  - Gönderici ile alıcı aralarında anahtar olarak SECRETKEY kelimesini belirlemiş olsunlar.
  - Gönderici bu anahtarı kullanarak şu metni şifrelesin: FLANK EAST ATTACK AT DAWN.

	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
A	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
B	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	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	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
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
F	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	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	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
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
J	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	i
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
L	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	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	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
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
T	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	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	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

F	L	A	N	K	E	A	S	T	A	T	T	A	C	K	A	T	D	A	W	N
S	E	C	R	E	T	K	E	Y	S	E	C	R	E	T	K	E	Y	S	E	C
X	P	C	E	O	X	K	U	R	S	X	V	R	G	D	K	X	B	S	A	P

	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
A	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
B	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	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	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
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
F	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	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	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
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
J	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	i
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
L	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	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	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
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
T	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	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	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

Şifreyi çözmek için ….

S	E	C	R	E	T	K	E	Y	S	E	C	R	E	T	K	E	Y	S	E	C
X	P	C	E	O	X	K	U	R	S	X	V	R	G	D	K	X	B	S	A	P
F	L	A	N	K	E	A	S	T	A	T	T	A	C	K	A	T	D	A	W	N

	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
A	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
B	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	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	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
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
F	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	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	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
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
J	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	i
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
L	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	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	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
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
T	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	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	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

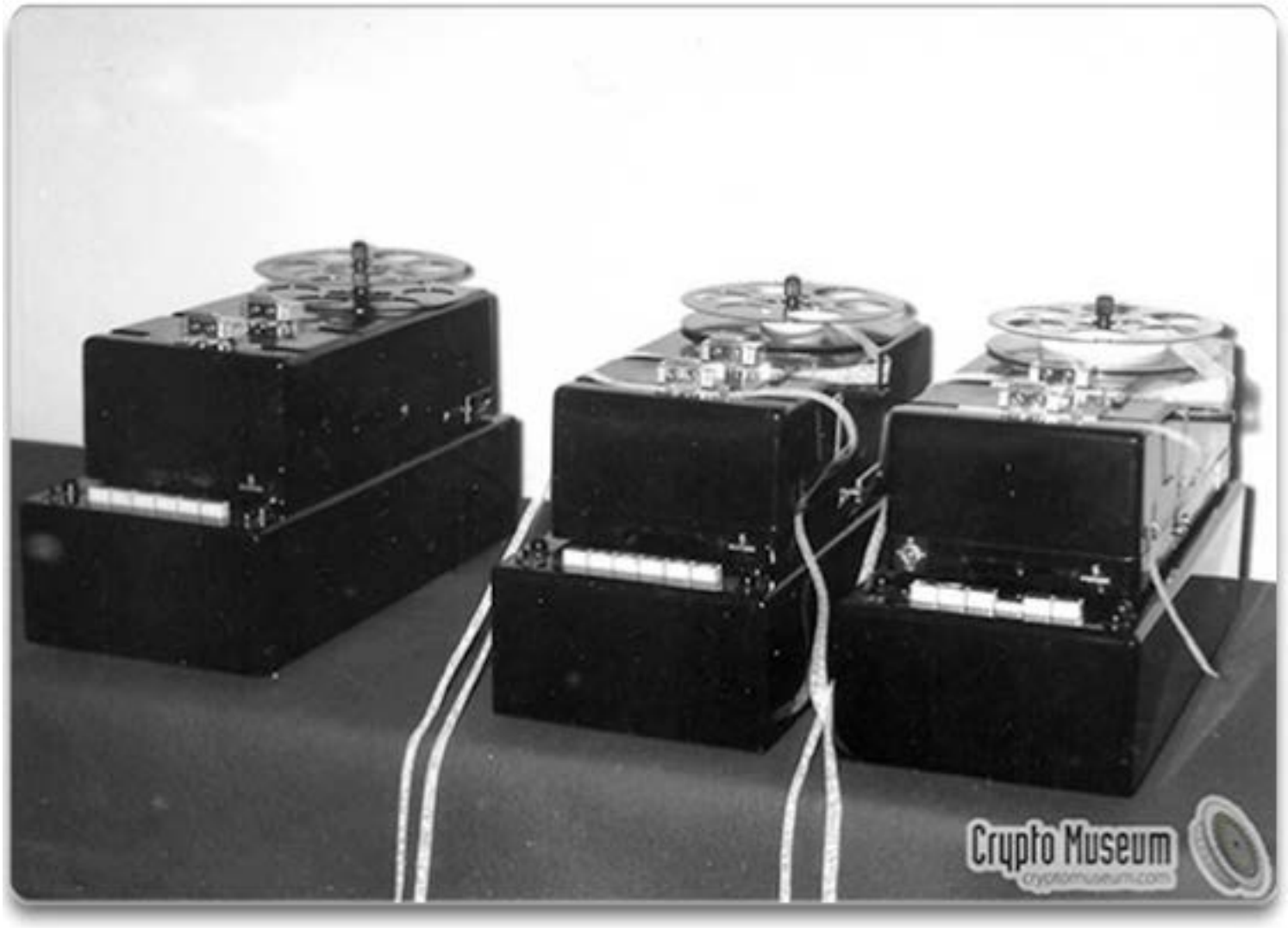
Devamını sen çöz….

T	C	P	I	P	T	C	P	I	P	T	C	P	I	P	T	C	P	I	P	T
V	E	C	I	H	X	E	J	Z	X	M	A									
C	C	N	A	S	E	C	U	R	I	T	Y									

Tek Kullanım Şifrelemesi

- 1917'de, Gilbert Vernam (AT&T Bell Labs mühendisi), akış şifrelemesini keşfetti ve patentini aldı.
  - Vernam tamamen rasgele üretilmiş veriyle aynı uzunlukta, birbirini kopyalayan dizilerden oluşmayan bir dizi üretmeyi önerdi.
  - Şifresiz metin bu dizi kullanılarak (XOR işlemi ile) şifrelenir.
  - Şifreyi çözmek için aynı dizi tekrar kullanılır.
- Her dizi sadece bir şifreleme işleminde kullanıldığı için tek kullanımlık şifre denilmiştir. Dizi tek kez kullanıldığı ve uzun olduğu için saldırılara karşı dayanıklı olur.

One-Time Pad Ciphers



Tek Kullanım Şifrelemesi

- Tek kullanım yönteminin uygulanmasında bazı zorluklar vardır.
  - Anahtar dağıtımı zordur.
  - Rasgele diziyi üretmek zordur ve birden çok kez kullanılırsa kırılma ihtimali artar.
- Bilgisayarlar dizilerin matematiksel özelliğinden dolayı doğru seriyi üretmekte zorlanırlar.
- RC4, internette yaygın kullanılan bir tek kullanım şifrelemesidir. Ancak anahtar bilgisayar tarafından üretilir ve gerçek anlamda rasgele değildir.

Cracking Code

- Secret key'i bilmeyen birinin şifreli mesajı belirlemeye çalışmasıdır.
- Kriptografinin kullanılmaya başladığı günden beri cracking de var.

Kriptanaliz

Cracking Code Yöntemleri

- Brute-Force Method
- Ciphertext-Only Method
- Known-Plaintext Method
- Chosen-Plaintext Method
- Chosen-Ciphertext Method
- Meet-in-the-Middle Method

Kriptanaliz
Brute-Force Attack

- Saldırgan decryption algoritmasıyla mümkün olan tüm kelimeleri çalışıncaya kadar dener. Tüm kriptolama algoritmaları bu saldırıya maruz kalabilir.
- Modern kriptografların amacı saldırganın şifreyi kırmasının çok uzun zaman almasını sağlayacak algoritmalar geliştirmektir.
- Örneğin: Sezar şifresiyle kriptolanan bir kodu kırmanın en iyi yolu brute-force atağıdır.
  - Sadece 25 mümkün dönüş söz konusudur.
  - Bu yüzden, mümkün olan tüm rotaları taraması fazla efor gerektirmez.

Brute-Force Attack

- Ortalama olarak tüm mümkün anahtarların % 50 si kadar denemeyle başarılabilir.
- DES cracking makinesi 56-bit DES anahtarıyla kodlanmış veriyi brute force ile 22 saatte kırar.
- Aynı metotla AES anahtarı 149 trilyon yılda kırılabiliyor.

Cryptanalysis
Methods for Cracking Code - Ciphertext-Only Attack

- An attacker has:
  - The ciphertext of several messages, all of which have been encrypted using the same encryption algorithm, but the attacker has no knowledge of the underlying plaintext.
  - The attacker could use statistical analysis to deduce the key.
- These kinds of attacks are no longer practical, because modern algorithms produce pseudorandom output that is resistant to statistical analysis.

Cryptanalysis
Methods for Cracking Code - Known-Plaintext Attack

- An attacker has:
  - Access to the ciphertext of several messages.
  - Knowledge (underlying protocol, file type, or some characteristic strings) about the plaintext underlying that ciphertext.
- The attacker uses a brute-force attack to try keys until decryption with the correct key produces a meaningful result.
- Modern algorithms with enormous keyspaces make it unlikely for this attack to succeed, because, on average, an attacker must search through at least half of the keyspace to be successful.

Cryptanalysis
Methods for Cracking Code - Chosen-Plaintext Attack

- An attacker chooses which data the encryption device encrypts and observes the ciphertext output. A chosen-plaintext attack is more powerful than a known-plaintext attack, because the chosen plaintext might yield more information about the key.
- This attack is not very practical, because it is often difficult or impossible to capture both the ciphertext and plaintext.

Cryptanalysis
Methods for Cracking Code - Chosen-Ciphertext Attack

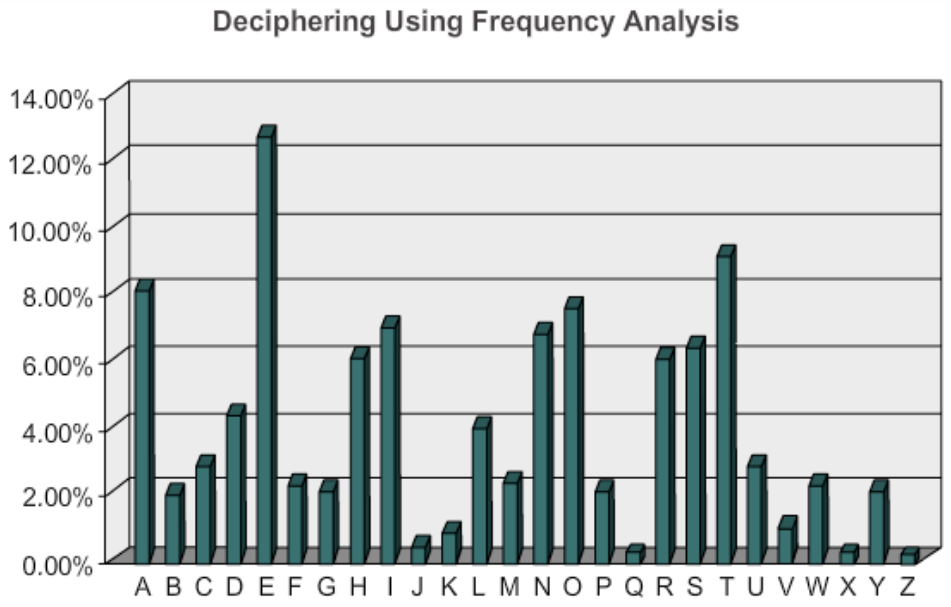
- An attacker chooses different ciphertext to be decrypted and has access to the decrypted plaintext. With the pair, the attacker can search through the keyspace and determine which key decrypts the chosen ciphertext in the captured plaintext.
- This attack is analogous to the chosen-plaintext attack.
  - Like the chosen-plaintext attack, this attack is not very practical.
  - Again, it is difficult or impossible for the attacker to capture both the ciphertext and plaintext.

Methods for Cracking Code - Meet-in-the-Middle

- The meet-in-the-middle attack is a known plaintext attack.
- The attacker knows that a portion of the plaintext and the corresponding ciphertext.
- The plaintext is encrypted with every possible key, and the results are stored. The ciphertext is then decrypted using every key, until one of the results matches one of the stored values.

Cracking Code Example

- The best way to crack the code is to use brute force.
- Because there are only 25 possible rotations, the effort is relatively small to try all possible rotations and see which one returns something that makes sense.
- A more scientific approach is to use the fact that some characters in the English alphabet are used more often than others.
- This method is called frequency analysis.



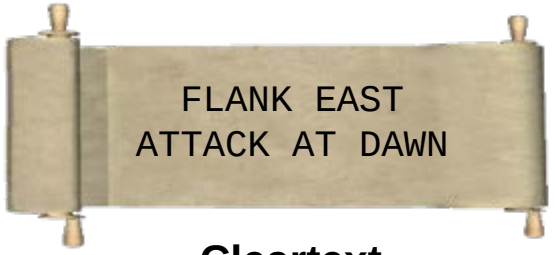
The graph outlines the frequency of letters in the English language.

For example, the letters E, T and A are the most popular.

Cracking Code Example- Frequency Analysis Method

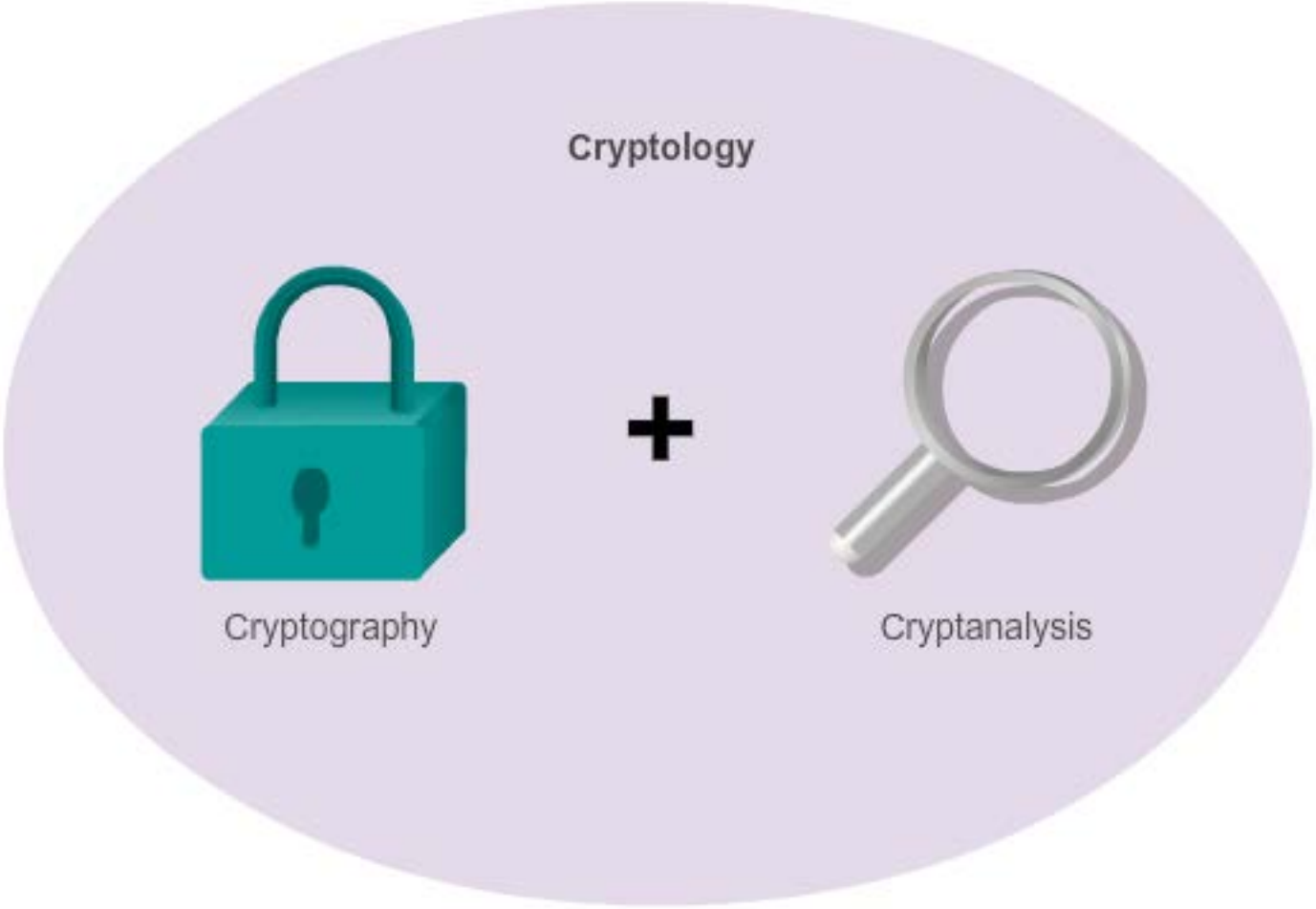
- The English alphabet is used more often than others.
  - E, T, and A are the most popular letters.
  - J, Q, X, and Z are the least popular.
- Caesar ciphered message:
  - The letter D appears six times.
  - The letter W appears four times.
  - Therefore, it is probable that they represent the more popular letters.
- In this case, D represents the letter A, and W represents the letter T.

Ciphered Text



Cleartext

Making and Breaking Secret Codes



Making and Breaking Secret Codes Cont.

- Cryptology is the science of making and breaking secret codes. It combines cryptography (development and use of codes), and cryptanalysis, (breaking of those codes).
- There is a symbiotic relationship between the two disciplines, because each makes the other one better.
  - National security organizations employ members of both disciplines and put them to work against each other.
- There have been times when one of the disciplines has been ahead of the other.
  - Currently, it is believed that cryptographers have the edge.

Cryptanalysis

- Ironically, it is impossible to prove an algorithm secure. It can only be proven that it is not vulnerable to known cryptanalytic attacks.
- There is a need for mathematicians, scholars, and security forensic experts to keep trying to break the encryption methods.
- Cryptanalysis are most used employed by:
  - Governments in military and diplomatic surveillance.
  - Enterprises in testing the strength of security procedures.

Sample Cryptanalysis Job Description

NSA

Cryptanalysis

National Security Agency | Fort Meade, MD

Job Description

Cryptanalysis is one of the core technical disciplines necessary for the NSA to accomplish its mission and provide critical intelligence to the nation's leaders. In an ever-changing global environment, the need for Cryptanalysts will remain constant.

Traditionally, Cryptanalysis is the art and science of solving cryptograms (writings in cipher or code) or cryptographic systems (devices for enciphering and deciphering) through analysis without prior knowledge of the encryption method. In a code, a word or phrase is replaced with another word, number, or symbol. In a cipher, each letter is replaced with another letter, number or symbol. Using known techniques and imagination, a Cryptanalyst systematically identifies basic elements in a cipher code that may lead to its solution. Modern Cryptanalysis includes analysis of any type of hidden information, whether a traditional cipher or a telecommunication protocol.

ANSWERING THE TOUGH QUESTIONS:

Cryptanalysts utilize mathematics, computer programming, engineering, and language skills as well as new technologies and creativity to solve tomorrow's problems today. That's why the NSA is looking for people who are intelligent and imaginative, and who can contribute original ideas to the solution of complex challenges. Cryptanalysts must communicate clearly, concentrate long and hard on difficult problems, and not be discouraged if success is elusive. No specific major is targeted for Cryptanalysis; the NSA hires people with technical and non-technical degrees, ranging from mathematics to music, engineering to history, and computer programming to chemistry.

The Secret Is in the Keys

Authentication, integrity, and data confidentiality are implemented in many ways using various protocols and algorithms. Choice depends on the security level required in the security policy.

	Integrity	Authentication	Confidentiality
Common cryptographic hashes, protocols, and algorithms	MD5 (weaker) SHA (stronger)	HMAC-MD5 HMAC-SHA-1 RSA and DSA	DES (weaker) 3DES AES (stronger)

The Secret Is in the Keys Cont.

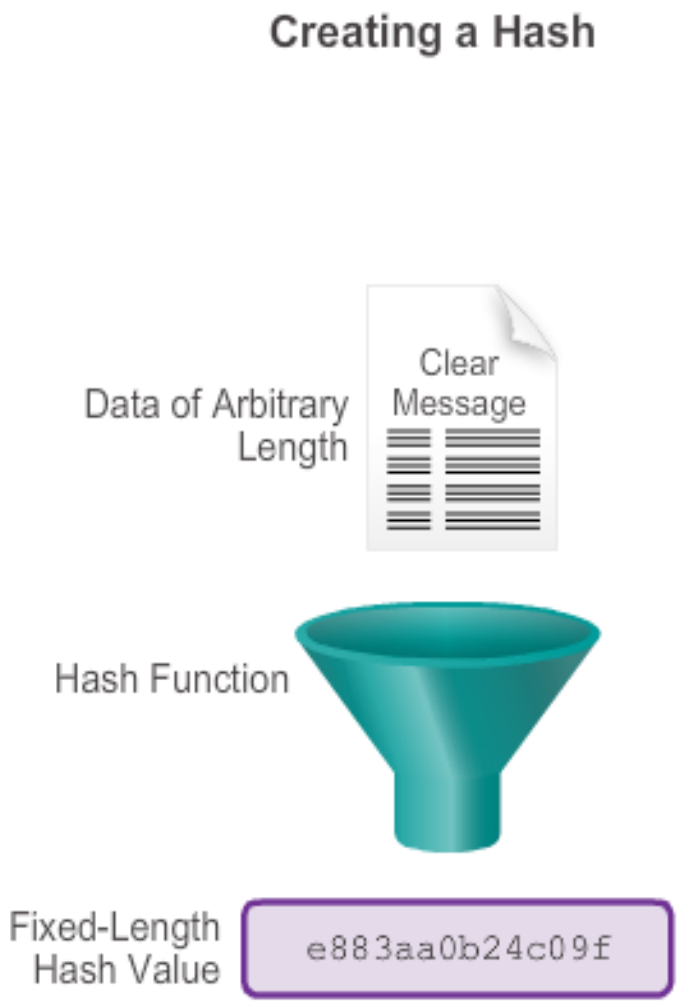
- Security of encryption lies in the secrecy of the keys, not the algorithm.
- Old encryption algorithms were based on the secrecy of the algorithm to achieve confidentiality.
- With modern technology, algorithm secrecy no longer matters since reverse engineering is often simple; therefore, public-domain algorithms are often used. Now, successful decryption requires knowledge of the keys.
- How can the keys be kept secret?

7.2 Temel Bütünlük ve Doğruluk

Cisco | Networking Academy®
Mind Wide Open™

Kriptografik Hash Fonksiyonu

- Bir hash fonksiyonu ikili mesajı alır ve karışık bir gösterimle çıkış üretir. Buna hash işlemi denir. Hash işlemi sonucu oluşan veriye hash değeri, mesaj özü veya sayısal parmak izi de denir.
- Hash işlemi, tek yönlü matematiksel bir fonksiyondur, hesaplaması kolaydır fakat geri elde edilmesi oldukça zordur.
- Hash işlemi veri bütünlüğü ve doğruluğundan emin olmak için kullanılır.



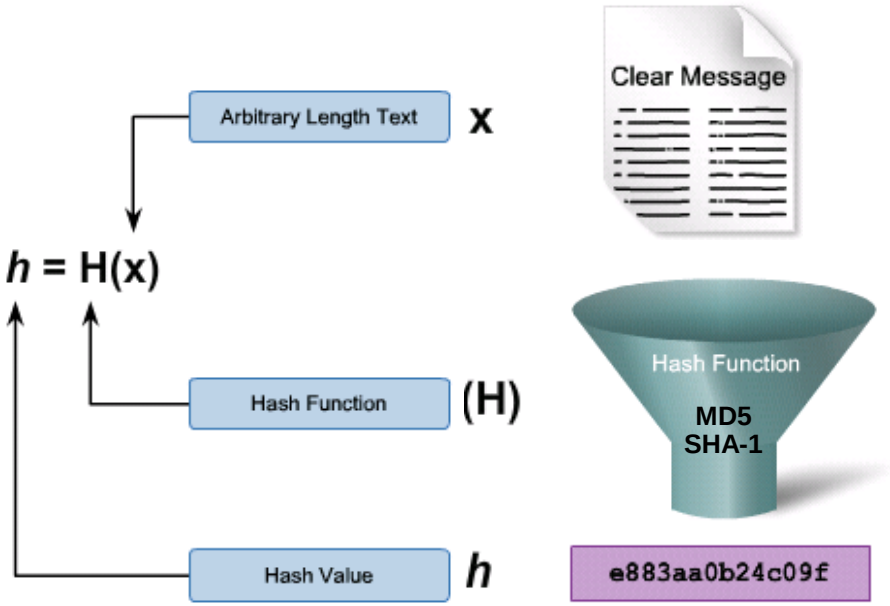
Kriptografik Hash Fonksiyonu

Kriptografik hash fonksiyonu çok farklı durumlarda uygulanır:

- Simetrik gizli anahtar kimlik doğrulamasında gizliliği doğrulamak için. IP Security (IPsec) veya routing protokol kimlik doğrulaması gibi.
- PPP CHAP gibi tek yönlü, tek kullanımlık kimlik doğrulama protokollerinde.
- Mesaj bütünlük doğrulamasında, güvenli web sitesi erişimi gibi.
- Download edilen dosyaların doğrulanmasında, Cisco IOS imajı gibi.

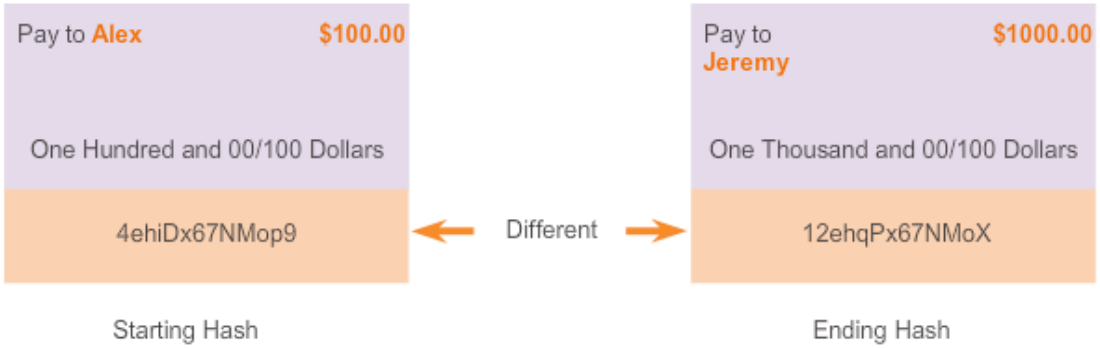
Kriptografik Hash Fonksiyonu Özellikleri

- Rasgele uzunlukta bir şifresiz mesajı alır.
- Hash fonksiyonuna koyar.
- Sabit boyutlu bir mesaj özü (hash değeri) üretir.
- H(x) :
  - Verilen x değeri için hesaplanması bilgisayar için kolaydır.
  - Tek yönlüdür ve geri dönülemez.
- Bir hash fonksiyonunu terse çevirmek zorsa, tek yönlü hash olarak kabul edilir.



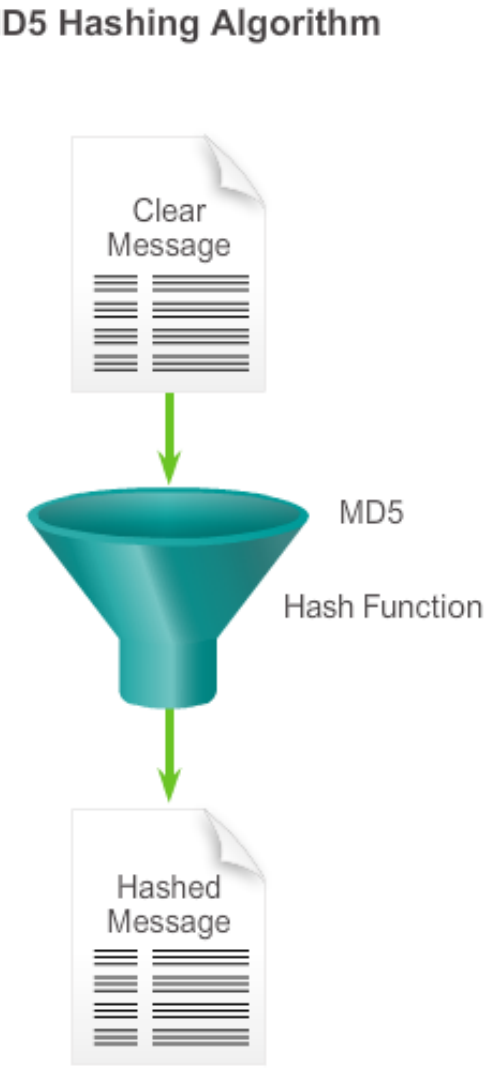
Yaygın Bilinen Hash Fonksiyonları

- Hash fonksiyonu, eğer veri iletim esnasında bozulmadıysa verinin doğrulanmasına yardımcı olur.
- Hash fonksiyonları kasti değişikliklere engel olamaz.
- Hashing prosedüründe göndericiden gelen bilginin içinde benzersiz tanımlayıcı yoktur. Böylece doğru hash fonksiyonuna sahip olmayan hiç kimse veriyi belirleyemez.
- Hashing, man-in-the-middle saldırılarına maruz kalabilir ve gönderilen verinin güvenliğini sağlamaz.
- İki iyi bilinen hash fonksiyonu:
  - MD5 128-bit karmaşıklıkla
  - SHA-256 256-bit karmaşıklıkla



Message Digest 5 Algoritması

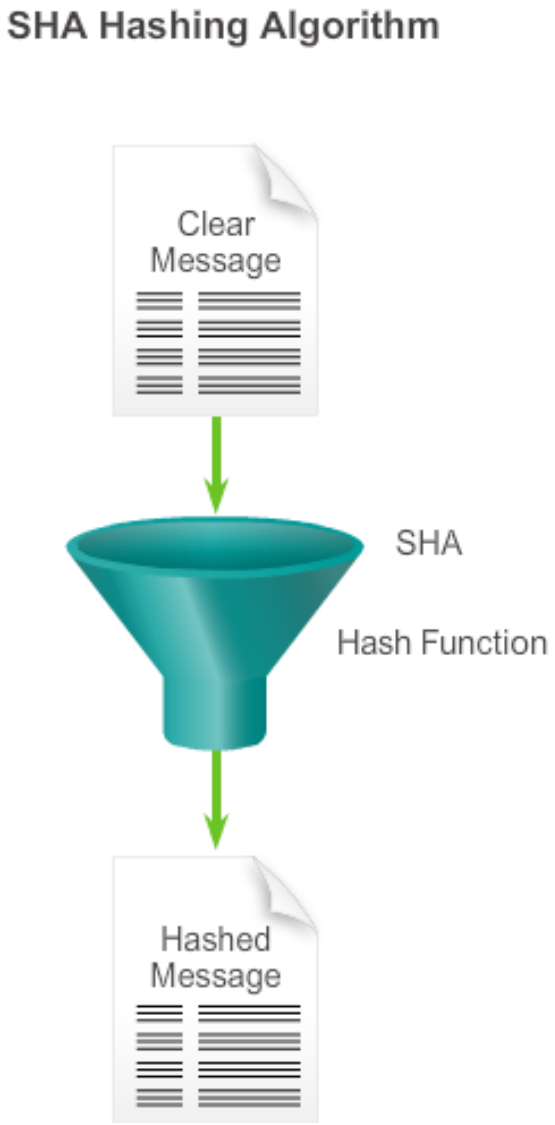
- Ron Rivest tarafından geliştirilmiştir.
- Günümüz internet uygulamalarında sıklıkla kullanılır.
- Tek yönlü hash fonksiyonudur. Hash değerinden verinin elde edilmesi çok güçtür.
- 512-bitlik mesaj bloklarını alıp hashler. Mesaj 512-bit değilse eklemelerle 512'nin katlarına tamamlanır.



MD5 ve SHA-1 ile Veri Bütünlüğü

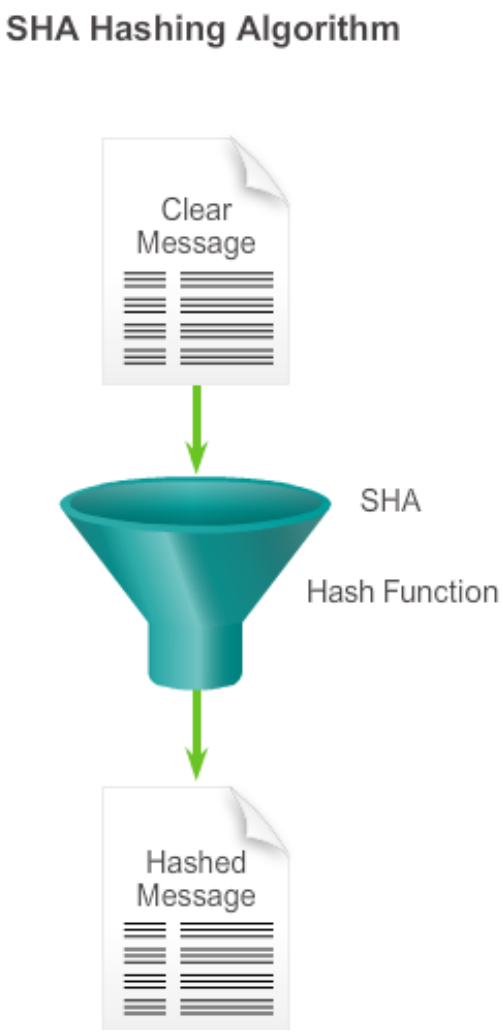
Secure Hash Algoritması

- NIST (National Institute of Standards and Technology) ve NSA (National Security Agency) kuruluslarinin ortak calismalari sonucunda 1994 yilinda Dijital Imza Standarti'nda (DSA-Digital Signature Standard) kullanilmak üzere tasarlanmis bir algoritmadir.
- MD5'e benzerlik göstermektedir.



Secure Hash Algoritması

- SHA-1 algoritması bir mesajı 2^64 bitten daha az olacak şekilde alır ve 160-bit mesaj özü üretir.
- MD5'den biraz daha yavaştır. Fakat üretim sonucu daha uzun olduğundan brute-force'a daha dayanıklıdır.
- NIST dört farklı SHA fonksiyonu daha yayınlamıştır:
  - SHA-224 (224 bit)
  - SHA-256 (256 bit)
  - SHA-384 (384 bit)
  - SHA-512 (512 bit)



MD5 - SHA-1 Karşılaştırması

MD5	SHA-1
Based on MD4	Based on MD4
Hesaplama 64 adımda yapılır	Hesaplama 80 adımda yapılır
MD5'in ciktisi 128-bit (4 adet 32 bitlik değişken kullanır)	SHA-1'in ciktisi 160-bit (5 adet 32 bitlik değişken kullanır)
Hızlı	Yavaş
Az Güvenilir	Çok Güvenilir

HMAC ile Gizlilik

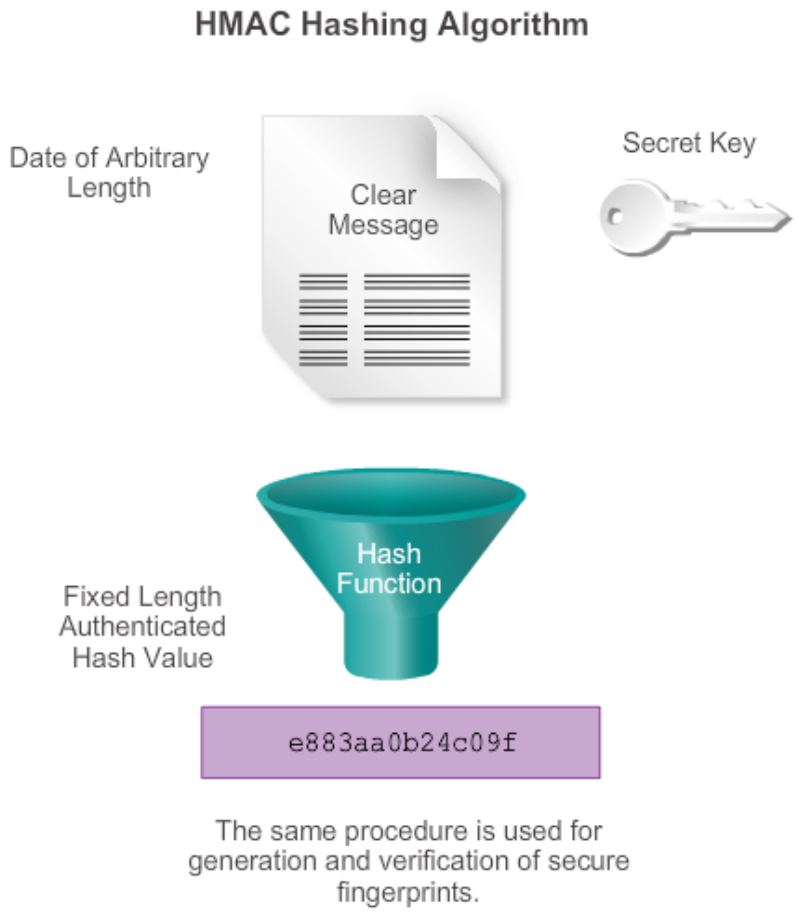
Keyed-Hash Message Authentication Code

- HMAC (veya KHMAC) bir mesaj kimlik doğrulama kodudur (message authentication code (MAC)). Bir hash fonksiyonu ve bir gizli anahtar kullanılarak hesaplanır.
  - HMAC, hash fonksiyonuna girdi olarak veriden başka bir de gizli anahtar alır.
  - Hash fonksiyonları, HMAC'in korunması esasına dayanır.
  - Hash fonksiyonunun çıkışı veri ve gizli anahtara bağlıdır.
- Gizlilik garanti edilmiş olur. Çünkü sadece gönderici ile alıcı gizli anahtarı bilir.
  - Sadece gönderici-alıcı HMAC özünü hesaplayabilir.
  - Bu özellik man-in-the-middle saldırılarına karşı koyar ve orijinal veri için kimlik doğrulama sağlar.

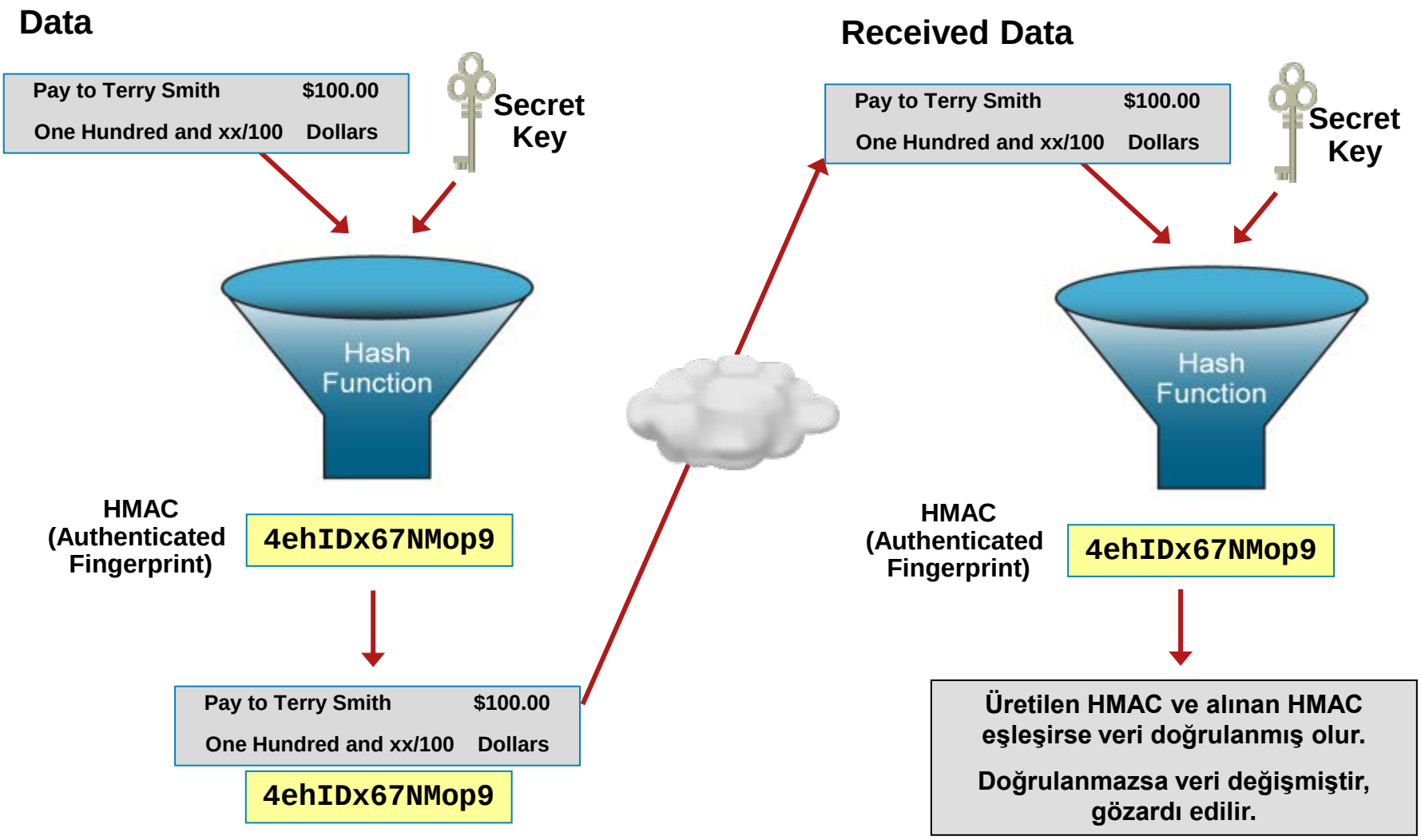
HMAC ile Gizlilik

Keyed-Hash Message Authentication Code

- HMAC'in kriptografik gücü şunlara bağlıdır:
  - Hash fonksiyonunun gücü.
  - Anahtarın kalitesi ve boyu.
  - Çıkış bitlerinin uzunluğu.
- Cisco iki iyi bilinen HMAC fonksiyonu kullanır:
  - Keyed MD5 veya HMAC-MD5 (MD5'i esas alır).
  - Keyed SHA-1 veya HMAC-SHA-1 (SHA-1'i esas alır).



HMAC İşlemleri



Anahtar Yönetimi Karakteristikleri

- Kriptografik sistemlerin en zor kısımlarından biri anahtar yönetimidir.
- Birkaç olmazsa olmaz karakteristik:
  - Key generation (anahtar üretimi)
  - Key verification (anahtar doğrulaması)
  - Key storage (anahtar depolama)
  - Key exchange (anahtar değişimi)
  - Key revocation and destruction (anahtar iptali ve yok edilmesi)

Anahtar Yönetimi Karakteristikleri

- **Key Generation**
  - Sezar kendi şifresi için anahtar değer seçer, gönderici/alıcı Vigenere gizli anahtarı seçer.
  - Modern kriptografi sistemleri anahtar üretimini otomatik olarak yapar.
- **Key Verification**
  - Hemen hemen tüm kriptografi sistemleri bazı zayıflıklara sahiptir. Bu anahtarlar kullanılmamalıdır (Sezar şifresinde 0 veya 25 dönüş gibi)
  - Anahtar doğrulama prosedürleri ile bu anahtarlar yeniden üretilebilirler.
- **Key Storage –** Modern kriptografi sistemleri anahtarları bellekte depolarlar.

Anahtar Yönetimi Karakteristikleri

- **Key Exchange**
  - Güvenilmez ortamlarda güvenli anahtar değişim prosedürleri sağlanmalıdır.
- **Key Revocation and Destruction**
  - Anahtarlar uzun süre kullanılamazlar. Eski anahtarlar silinmelidir. Bu sayede saldırganlar eski anahtarları saldırı için kullanamaz.
- Anahtarı tanımlamak için iki terim kullanılır:
  - **Key size** – Anahtar içindeki bit sayısıdır.
  - **Keyspace –** Mümkün olan anahtar sayısıdır.

Anahtar Yönetimi Karakteristikleri

- Anahtar uzunluğu artarkan keyspace üstel olarak artar:
  - 2^2 key = a keyspace of **4**
  - 2^3 key = a keyspace of **8**
  - 2^4 key = a keyspace of **16**
  - 2^{40} key = a keyspace of **1,099,511,627,776**

Keyspace

- Anahtara bir bit ekleme keyspace'i iki katına çıkarır.
- DES anahtarına bir bit eklenmiş olması saldırganın keyspace'i çözmesi için iki kat zamana ihtiyacı olması anlamına gelir.
- Uzun anahtar daha güvenlidir ancak çok kaynak tüketir.

DES Key Length	Keyspace	# of Possible Keys
56 bit	2^{56}	72,000,000,000,000,000
57 bit	2^{57}	144,000,000,000,000,000
58 bit	2^{58}	288,000,000,000,000,000
59 bit	2^{59}	576,000,000,000,000,000
60 bit	2^{60}	1,152,000,000,000,000,000

Kriptografik Anahtar Türleri

- Simetrik anahtarlar VPN destekleyen iki router arasında kullanılabilir.
- Asimetrik anahtarlar HTTPS uygulamalarında kullanılır
- Güvenli web sayfasına bağlanıldığında dijital imzalar kullanılır
- Hash anahtarları simetrik ve asimetrik anahtar üretiminde, dijital imzalarda ve diğer uygulamalarda kullanılır

	Symmetric Key	Asymmetric Key	Digital Signature	Hash
Protection up to 3 years	80	1248	160	160
Protection up to 10 years	96	1776	192	192
Protection up to 20 years	112	2432	224	224
Protection up to 30 years	128	3248	256	256
Protection against quantum computers	256	15424	512	512

Kriptografik Anahtarların Seçimi

- Kısa anahtarlar hızlı işlem görür ancak az güvenilirdir.
- Uzun anahtarlar yavaş işlem görür ancak daha güvenlidir.
- Yönetici ikisi arasında bir denge kullanmalıdır.

Shorter keys equal faster processing, but are less secure.

Longer keys equal slower processing, but are more secure.

7.3 Gizlilik

Cisco | Networking Academy®
Mind Wide Open™

Kriptografik Şifreleme

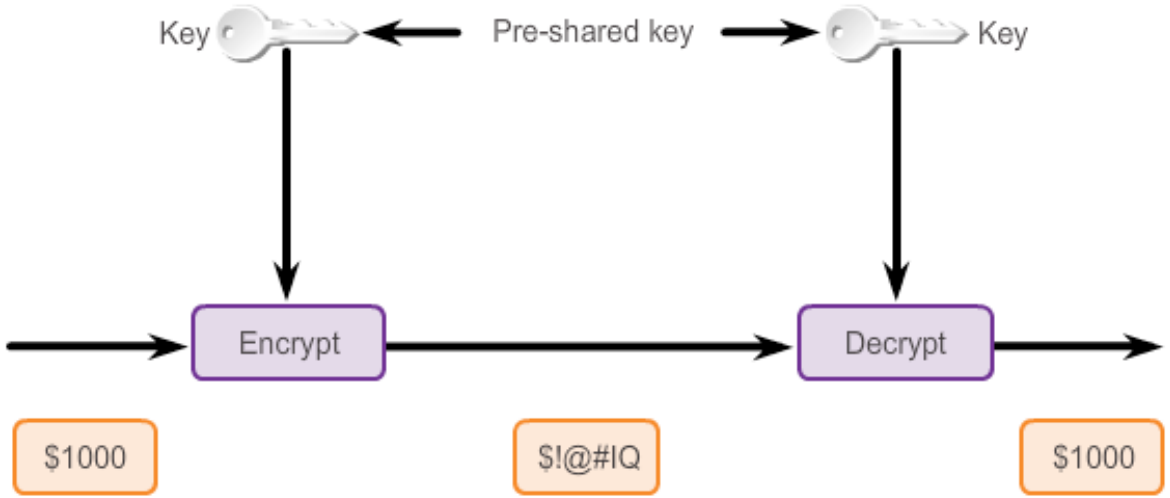
Kriptografik şifreleme çeşitli protokol ve araçlar kullanarak OSI modelinin birkaç katmanında gizlilik sağlayabilir:

- Uygun link-kriptolama cihazları veri-bağlantı katmanı gizliliği sağlar.
- Ipsec gibi protokol yığınları gibi network katmanı protokolleri, network katmanı gizliliği sağlar.
- Secure Sockets Layer (SSL) veya Transport Layer Security (TLS), oturum katmanı gizliliği sağlar.
- Güvenli email, güvenli database session (Oracle SQL*net) ve güvenli mesajlaşma (Lotus Notes sessions) gibi uygulamalar uygulama katmanı gizliliği sağlar.

Simetrik Kriptolama Algoritmaları

Simetrik Kriptolama Algoritmaları aşağıdaki karakteristiklere sahiptir:

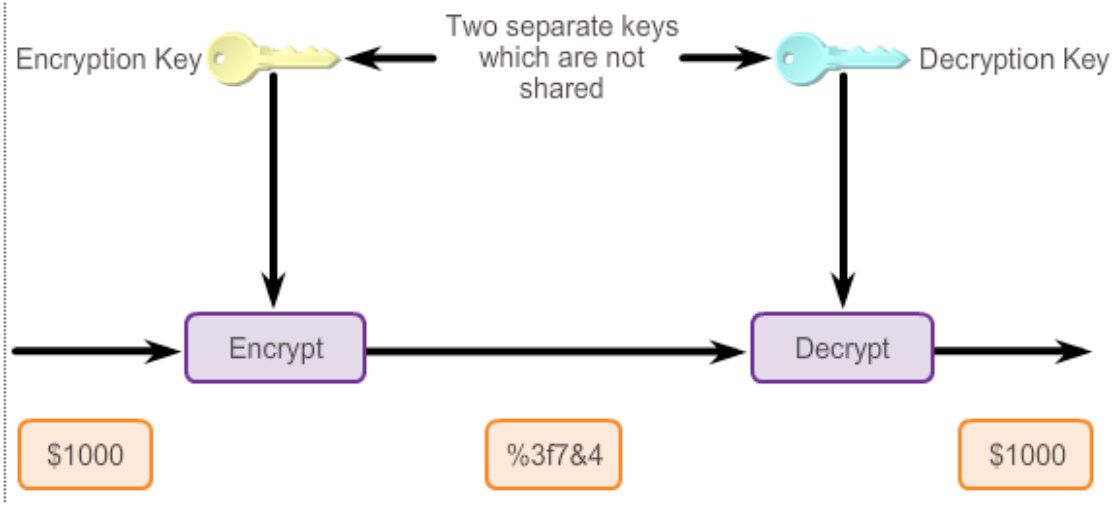
- Shared-secret key (paylaşılmış gizli anahtar) algoritmaları olarak bilinirler.
- Kullanışlı anahtar uzunluğu 80-256 bit arasıdır.
- Gönderici ve alıcı bir gizli anahtarı aralarında paylaşırlar.
- Genellikle çok hızlıdırlar (kablo hızında) çünkü bu algoritmalar basit matematiksel işlemlere dayanır.
- DES, 3DES, AES, IDEA, RC2/4/5/6 ve Blowfish bu algoritmalara örnektir.



Asimetrik Kriptolama Algoritmaları

Asimetrik Kriptolama Algoritmaları şu karakteristiklere sahiptir:

- Public key (genel anahtar) algoritmaları olarak bilinirler.
- Kullanışlı anahtar uzunlukları 512-4,096 bit arasıdır.
- Gönderici ve alıcı gizli anahtar paylaşmazlar.
- Bu algoritmalar simetriklere nazaran daha yavaştır. Çünkü zor hesaplamalar içerirler.
- RSA, ElGamal, elliptic curves ve DH algoritmaları asimetrik algoritmalardır.



Simetrik Kriptolama Algoritmaları

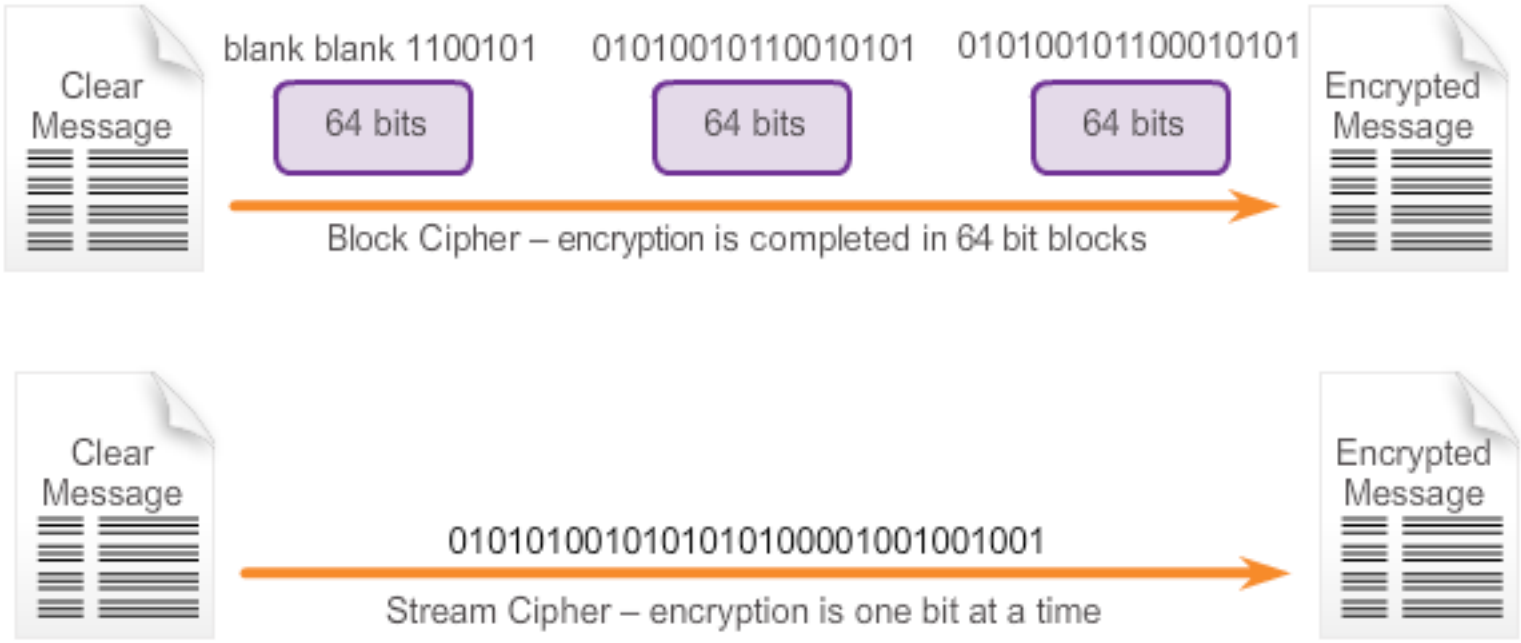
- Aynı zamanda paylaşılmış anahtar algoritmaları olarak bilinirler. Önceden paylaşılmış gizli anahtar kullanılarak şifreleme ve şifre çözme işlemi yapılır. Pre-shared key kriptolu haberleşme başlamadan önce bilinir.
- Alıcı-gönderici gizli anahtarı korurlar ve hızlıca enkript-dekript işlemi yaparlar. Çünkü anahtar boyutu kısadır
- Bu yüzden simetrik algoritmalar az işlem yükü getirir.

Symmetric Encryption Algorithm	Key length (in bits)
DES	56
3DES	112 and 168
AES	128, 192, and 256
Software Encryption Algorithm (SEAL)	160
The RC series	RC2 (40 and 64) RC4 (1 to 256) RC5 (0 to 2040) RC6 (128, 192, and 256)

Simetrik Kriptolama Teknikleri

İki kriptolama yöntemi kullanılır:

- Blok Cipher
- Stream Cipher

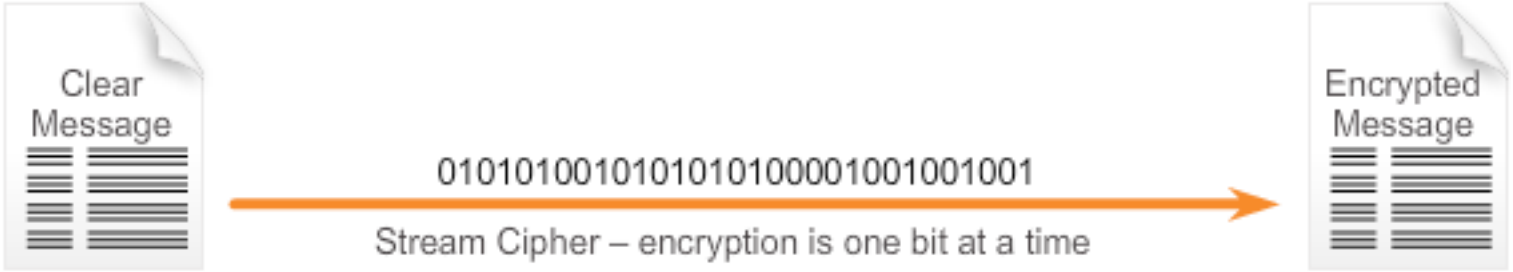


Simetrik Kriptolama Teknikleri

- Blok cipher, sabit uzunluklu şifresiz metini 64 veya 128 bitlik bloklara dönüştürür.
  - Blok boyutu ne kadar verinin bir anda şifreleneceğini ifade eder.
  - Anahtar uzunluğu ise kullanılan gizli anahtarın uzunluğunu ifade eder.
  - Şifrelenmiş metin aynı anahtar kullanılıp ters dönüşüm uygulanarak dekript edilir.
- Yaygın kullanılan blok cipher'lar:
  - DES 64-bit block size
  - AES 128-bit block size
  - RSA değişken block size

Simetrik Kriptolama Teknikleri

- Stream cipher, şifresiz metnin bir anda bir bitini veya bir byte'ını kriptolar.
  - Bu yöntem blok boyutu bir bit olan blok cipher olarak düşünülebilir.
  - Vigenère cipher , stream cipher'a örnektir.
  - Blok cipher'dan daha hızlı çalışabilir ve mesaj boyunu artırmaz.
- Yaygın kullanılan stream cipher yöntemleri:
  - A5, GSM telefon haberleşmesini şifreler.
  - RC4.
  - DES, stream cipher'da da uygulanabilir.



Kriptolama Algoritması Seçimi

- Kriptoloji dünyasında algoritma güvenilir mi?
- Kullanılan algoritmanın uzun yıllar saldırılara direnebilmesi istenir.
- Algoritma brute-force ataklarına yeterince dirençli mi? Uygun anahtar boyutlarıyla bu ataklar savuşturulabilir.
- Algoritma değişken ve uzun boyutlu anahtarları destekliyor mu?
- Algoritma kısıtlara sahip mi?

Kriptolama Algoritması Seçimi

	DES	3DES	AES
Kriptoloji dünyasında algoritma güvenilir mi?	3DES'le değiştirildi	Evet	Henüz karar verilmedi
Algoritma brute-force saldırılarına dayanıklı mı?	Hayır	Evet	Evet

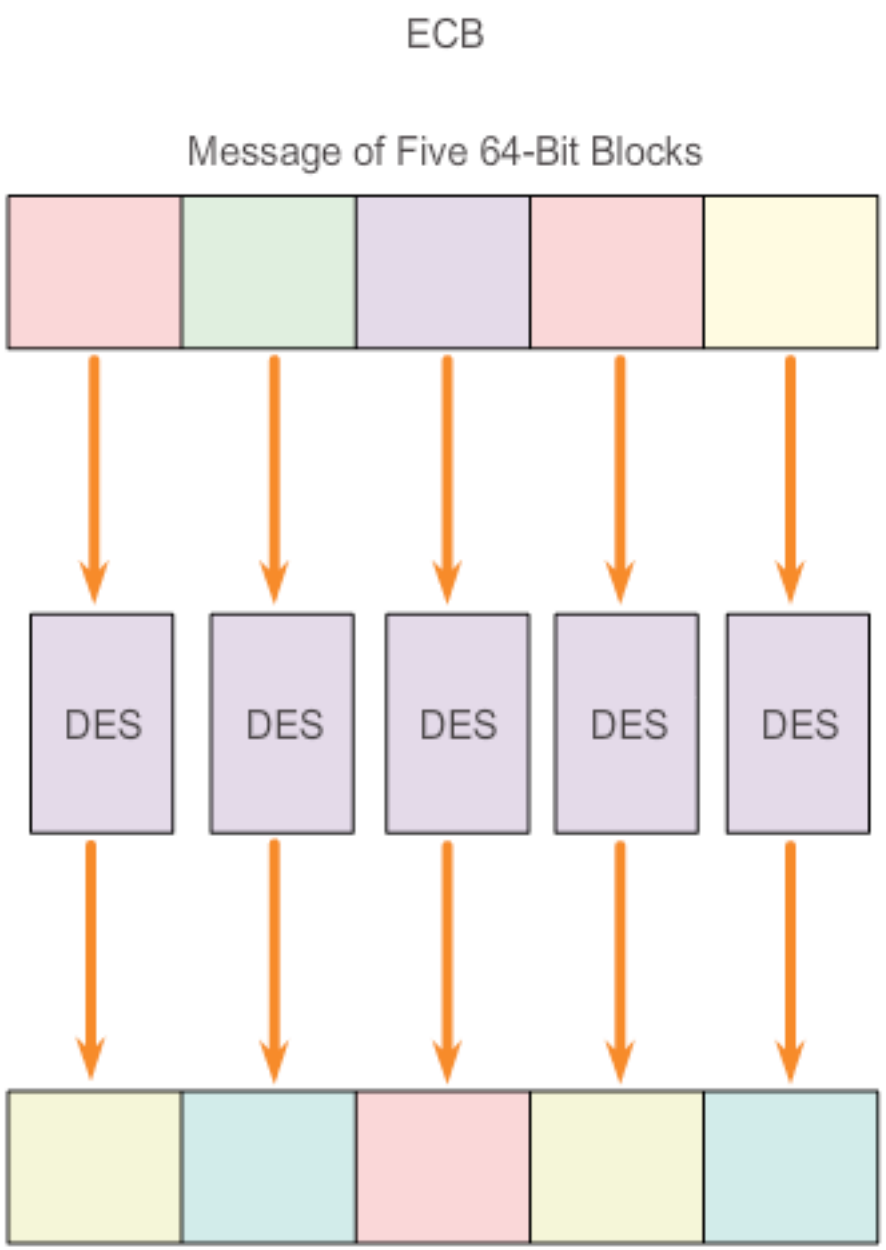
DES Simetrik Kriptolama

- En popüler simetrik kriptolama standardıdır.
  - IBM tarafından geliştirilmiştir
  - 1970'lerde kırılamaz olduğu düşünülüyordu
  - Paylaşılmış anahtar kriptolama ve çözme sağlar
- DES, 64-bitlik şifresiz metin bloklarını kriptolama algoritması ile şifreli metinlere dönüştürür.

DES Characteristics	
Description	Data Encryption Standard
Timeline	Standardized 1976
Type of Algorithm	Symmetric
Key size (in bits)	56 bits
Speed	Medium
Time to crack (Assuming a computer could try 255 keys per second)	Days (6.4 days by the COPACABANA machine, a specialized cracking device)
Resource Consumption	Medium

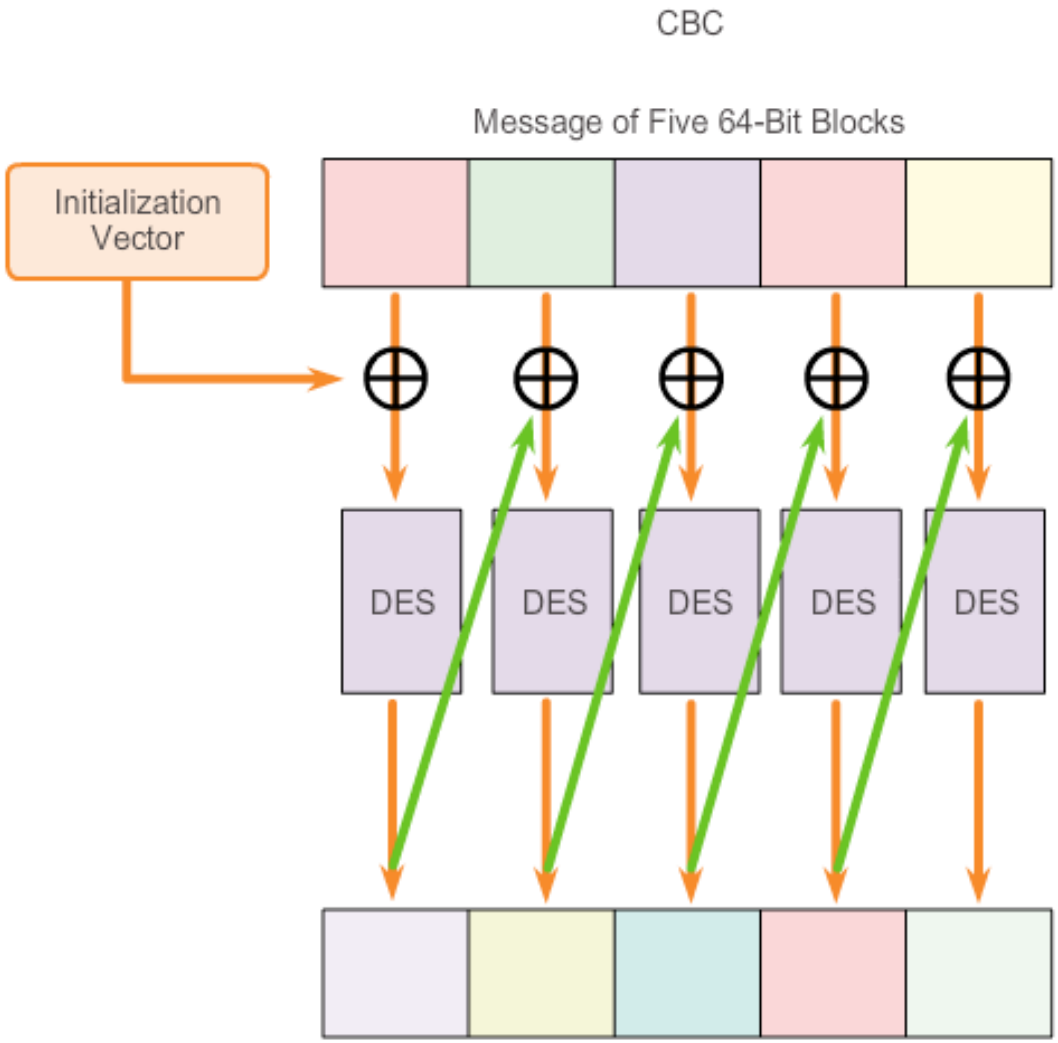
DES İşlemleri

- ECB (Electronic Code Book) modu seri olarak her bir 64-bitlik şifresiz metni, 56-bitlik anahtar kullanarak şifreler.
- Eğer iki aynı blok benzer anahtarlar kullanılarak kriptolanırsa onların ciphertext halleri de benzer olur.
- Bu yüzden bir saldırgan benzer veya aynı trafik akışından belirleme yapabilir.



DES İşlemleri

- CBC (Cipher Block Chaining) modunda, her bir 64-bitlik açık metin, önceki şifreli metin blokuyla bit bazında XOR işlemine tabi tutulur, ardından DES anahtarıyla şifrelenir.
- Her blokun kriptolanması önceki bloklara bağlıdır.
- Aynı 64-bitlik bloklar farklı şifreli metinlere dönüşmüş olur.



DES İşlemleri

- 64-bitten daha büyük verileri şifreleme veya çözme için DES iki yaygın akış modu kullanır:
  - Cipher feedback (CFB), CBC'ye benzer ve her hangi bir sayıdaki biti kriptolayabilir, tek bir bit veya tek bir karakter bile olabilir.
  - Output feedback (OFB) anahtar akış blokları üretir. Bunlar şifresiz metinle XOR'lanır.
- Cipher önceki ciphertext'i ve gizli anahtarı kullanarak yalancı rasgele bit akışları üretir.

DES Özet

- Kısa anahtar uzunluğu sayesinde DES veriyi korumak için kısa sürede sonuca giden bir protokol olarak davranır.
  - 3DES, DES'e nazaran daha iyi koruma sağlar. Çünkü daha güvenilir ve daha güçlü güvenlik özelliklerine sahiptir.
- Tavsiyeler:
  - Anahtarın sıklıkla değiştirilmesi brute-force ataklarına direnç sağlar.
  - Güvenli bir kanal kullanılarak DES anahtarı gönderici alıcı arasında paylaştırılmalıdır.
  - CBC modda çalışan DES kullanılmalıdır.
  - Anahtar zayıfsa kullanılmadan önce test edilmelidir.

DES'in gelişmişi: 3DES

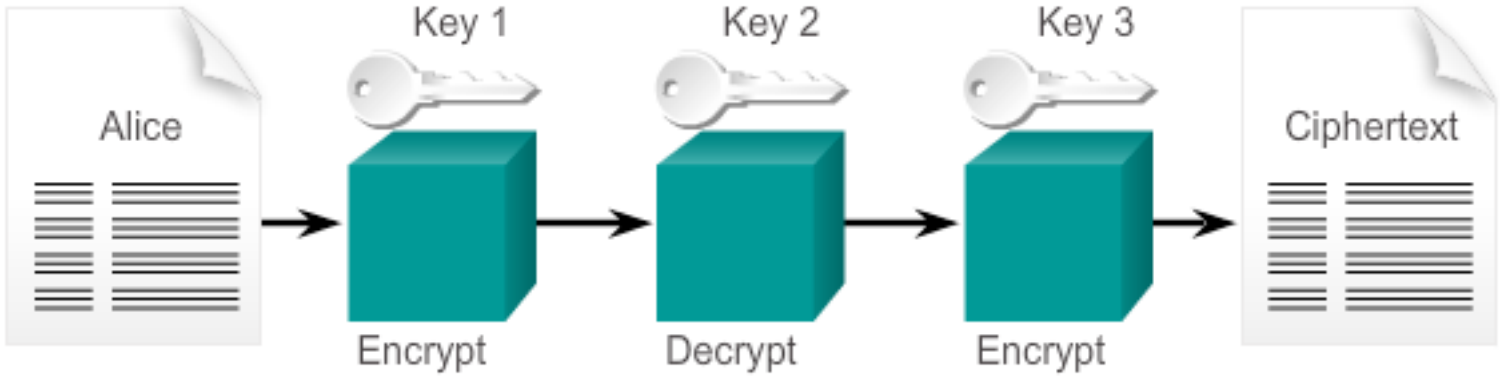
- 3DES, DES'in 256 kat güçlendirilmiş halidir.
- 64-bitlik veri bloklarını alır ve 3 kez DES işlemine tabi tutar:
  - Kriptolama, çözme ve kriptolama.
  - İlave işlem zamanına ihtiyaç duyar.
  - 1,2 veya 3 farklı DES anahtarı kullanabilir (1 anahtar kullanıldığında DES'in aynısı olur).

DES'in gelişmişi: 3DES

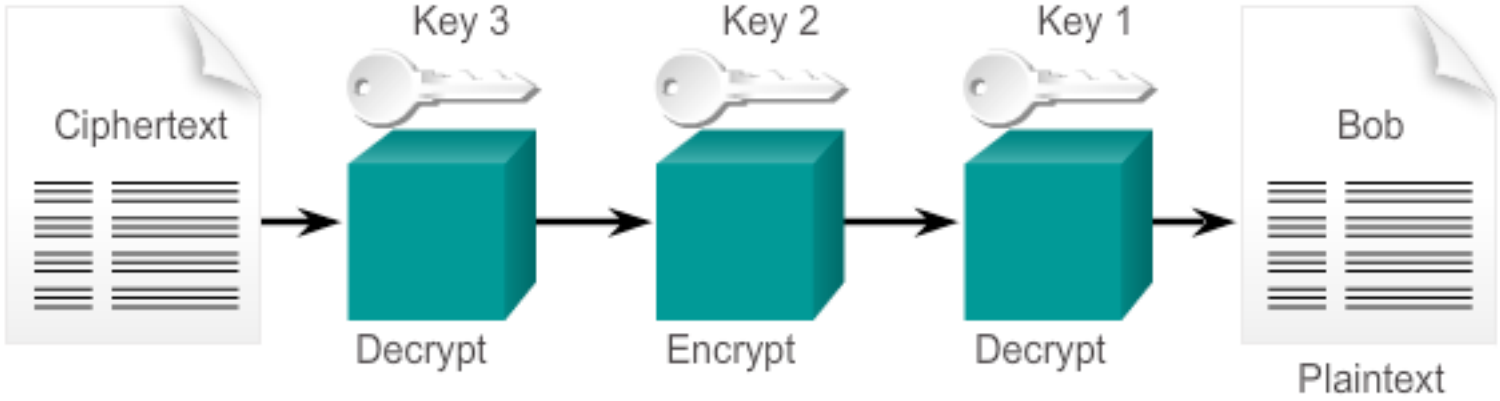
3DES Characteristics	
Description	Triple Data Encryption Standard
Timeline	Standardized 1977
Type of Algorithm	Symmetric
Key size (in bits)	112 and 168 bits
Speed	Low
Time to crack (Assuming a computer could try 255 keys per second)	4.6 Billion years with current technology
Resource Consumption	Medium

3DES İşlemleri

3DES Encryption



3DES Decryption



Advanced Encryption Standard (AES)

AES

- 1997'de, AES'in ilk hali ilan edildi. Ve kriptolama şeması DES ile değiştirildi.
- 5 yıllık standartlaşma süresinin sonunda 15 öneri yarıştı ve National Institute of Standards and Technology (NIST) tarafından Rijndael'in blok şifresi AES algoritması olarak seçildi.
  - Rijndael ("Rhine dahl") algoritmasını esas alır.
  - 128, 192, veya 256 bit uzunluğunda blokları 128, 192 veya 256 bit şifrelerle kodlar.
  - 9 farklı kombinasyonun tümü kullanılabilir.
- AES, son Cisco router IOS imajlarında aktiftir.

AES Özet

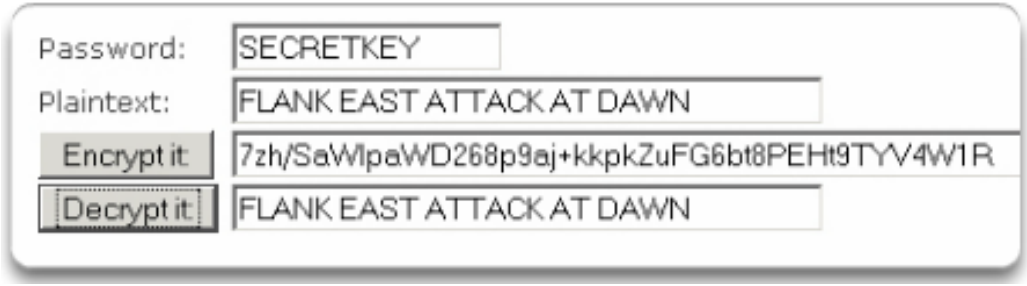
- AES şu sebeplerden dolayı DES yerine tercih edilebilir:
  - AES anahtar uzunluğundan dolayı DES'ten daha güçlüdür.
  - AES, aynı donanım üzerinde 3DES'ten daha hızlı çalışır.
  - AES high-throughput, low-latency açılarından daha kullanışlıdır, özellikle yazılımla kriptolama kullanılıyorsa.
- Ancak, AES genç bir algoritmadır ve kriptografinin altın kuralına göre algoritma kemale ermiş olmalıdır.
- Bu açıdan 3DES 40 yıllık ve test edilmiş bir algoritmadır.

AES Özet

In this example,the SECRETKEY key and plaintext are entered.

They are now encrypted using 128 AES.

An attempt at deciphering the text using a lowercase, and incorrect key.



A second attempt at deciphering the text using the correct key displays the original plaintext.

Software-Optimized Encryption Algorithm (SEAL)

SEAL Scorecard

SEAL Characteristics	
Description	Software-Optimized Encryption Algorithm
Timeline	First published in 1994. Current version is 3.0 (1997)
Type of Algorithm	Symmetric
Key size (in bits)	160
Speed	High
Time to crack (Assuming a computer could try 255 keys per second)	Unknown but considered very safe
Resource Consumption	Low

RC Algoritmaları

- RC algoritmaları tümüyle veya büyük kısımları MD5'i de geliştirilen Ronald Rivest tarafından geliştirilmiştir.
- Hız ve değişken anahtar boyu özelliklerinden dolayı network uygulamalrında kullanılır.
- Farklı varyasyonları vardır:
  - RC2
  - RC4
  - RC5
  - RC6

RC Algoritmaları

RC Algorithms Scorecard

Ron's Code or Rivest Codes Scorecard		
Description	RC2	RC4
Timeline	1987	1987
Type of Algorithm	Block cipher	Stream cipher
Key size (in bits)	40 and 64	1 - 256

Ron's Code or Rivest Codes Scorecard		
Description	RC5	RC6
Timeline	1994	1998
Type of Algorithm	Block cipher	Block cipher
Key size (in bits)	0 to 2040 bits (128 suggested)	128, 192, or 256

Diffie-Hellman (DH) Algoritması

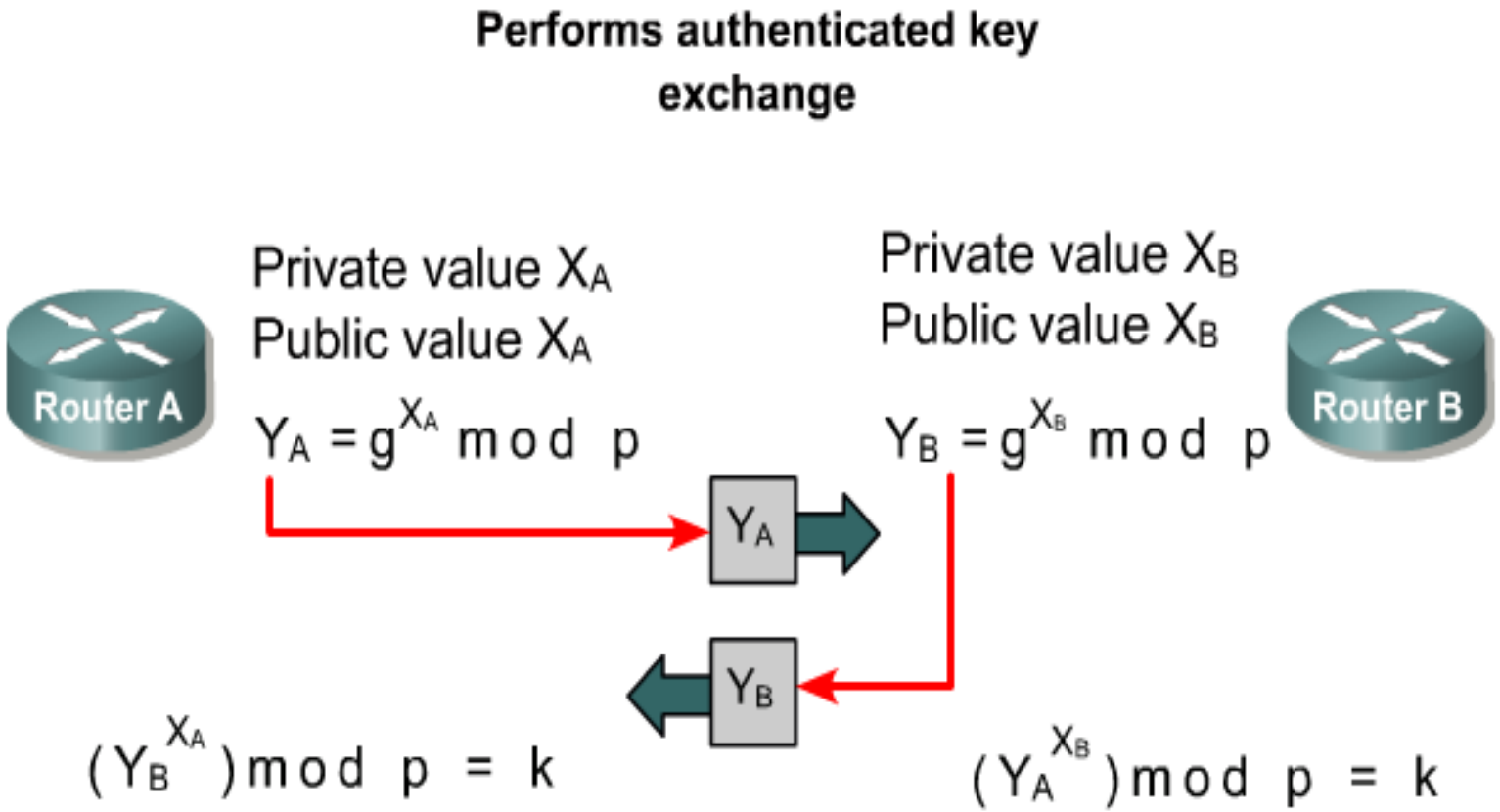
- Whitfield Diffie ve Martin Hellman tarafından 1976'da geliştirilmiştir.
- DH, en modern otomatik anahtar değiştirme algoritmasına dayanır ve network alanında en yaygın kullanılan protokoldür.
- DH bir kriptolama mekanizması DEĞİLDİR. Veriyi kriptolama için kullanılmaz.
  - Anahtarı değiş tokuş yapmak için kullanılan bir metottur.
  - Bu anahtar simetrik anahtar şifrelemede kullanılır

Diffie-Hellman (DH) Algoritması

- DH özellikle veri Ipsec VPN ile iletildiğinde kullanılır. Veri internet üzerinde SSL veya TLS ile ile şifrelenir.

Description	Diffie-Hellman Algorithm
Timeline	1976
Type of Algorithm	Asymmetric
Key size (in bits)	512, 1024, 2048
Speed	Slow
Time to crack (Assuming a computer could try 255 keys per second)	Unknown but considered very safe
Resource Consumption	Medium

DH İşlemleri



DH İşlemleri

Ali ve Veli'nin DH Anahtar Değişimi

Ali		
Shared	**Secret**	**Calc**
5, 23		
	6	$5^6 \bmod 23 = 8$

Veli		
Shared	**Secret**	**Calc**
5, 23		

- Veli ile Ali base number g=5 ve prime number p=23 kullanmak üzere anlaşır
  - Ali secret integer a=6 seçer
  - Ali Veli'ye ($g^a \bmod p$) yani $5^6 \bmod 23 = 8$ değerini gönderir.

DH İşlemleri

Modulo

- Hesaplamada modül alma işlemi yapılır.

DH İşlemleri

Ali ve Veli'nin DH Anahtar Değişimi

Ali		
Shared	**Secret**	**Calc**
5, 23		
	6	$5^6 \bmod 23 = 8$
		$19^6 \bmod 23 = 2$

Veli		
Shared	**Secret**	**Calc**
5, 23		
	15	$5^{15} \bmod 23 = 19$
		$8^{15} \bmod 23 = 2$

- Bu arada Veli secret integer b =15 seçer.
- Veli Ali'ye, $(g^a \bmod p) = 5^{15} \bmod 23 = 19$ gönderir.
- Ali $(x^a \bmod p) = 19^6 \bmod 23 = 2$ değerini hesaplar.
- Veli $(x^a \bmod p) = 8^6 \bmod 23 = 2$ değerini hesaplar.

DH İşlemleri

Ali ve Veli'nin DH Anahtar Değişimi

Ali		
Shared	**Secret**	**Calc**
5, 23		
	6	$5^6 \bmod 23 = 8$
		$19^6 \bmod 23 = 2$

Veli		
Shared	**Secret**	**Calc**
5, 23		
	15	$5^{15} \bmod 23 = 19$
		$8^{15} \bmod 23 = 2$

- Sonuç (2) Ali ve Veli için eşittir.
- Onlar şifreleme için bu gizli anahtarı şifreleme için kullanırlar.

Diffie-Hellman Key Exchange

DH İşlemleri

Ali ile Veli’nin anahtar değişimi

Başlangıç gizli tamsayısı Ali için(**6**) ve Veli için (**15**) değerleri 1024 bitlik çok uzun değerlerdir.

8 bit = 10101010

1,024 bit =

101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101010
1010101010101010101010101010101010101010101010101010101010101010