Şifreleme Algoritmalarının Sınıflandırılması ve Algoritmalara Saldırı Teknikleri

Yrd.Doç.Dr.Mehmet Tektaş

Kriptografi: Gizli mesajlaşma, onaylama, dijital imzalar, elektronik para ve diğer uygulamaların tümüyle ilgili bilim dalıdır.

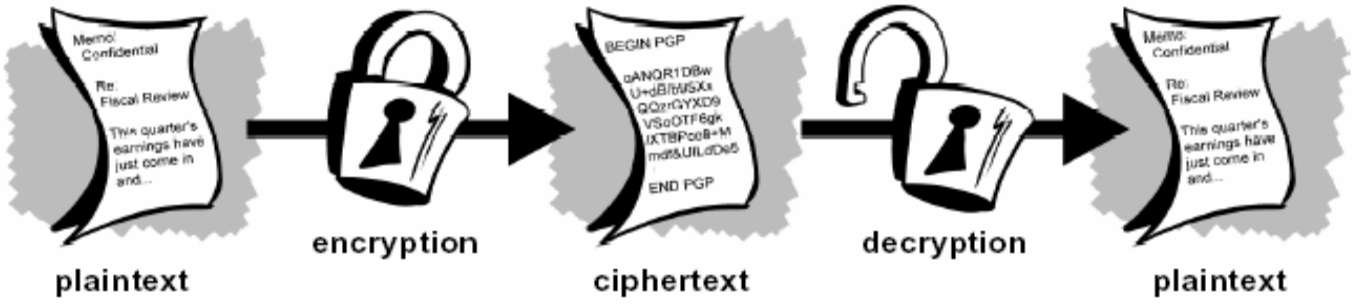
Kriptoloji: Kriptografik metotların matematiksel temelleriyle ilgilenen bir matematik dalıdır

Kriptoanaliz : Kriptografik algoritmaların açıklarını bulup ortaya çıkartmaya ise kriptoanaliz denilmektedir.

Şifreleme Algoritmaları

- Geçmişte ilgilenilen kriptografi algoritmaları algoritmanın gizliliğine dayanmaktaydı. Günümüzde kullanılmakta olan modern ve güçlü şifreleme algoritmalar ise artık gizli değildir. Bu algoritmalar güvenliklerini kullandıkları farklı uzunluk ve yapılardaki anahtarlarla sağlarlar. Bütün modern algoritmalar şifrelemeyi ve şifre çözmeyi kontrol için anahtarları kullanır.

Temel Kriptoloji Terimleri



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

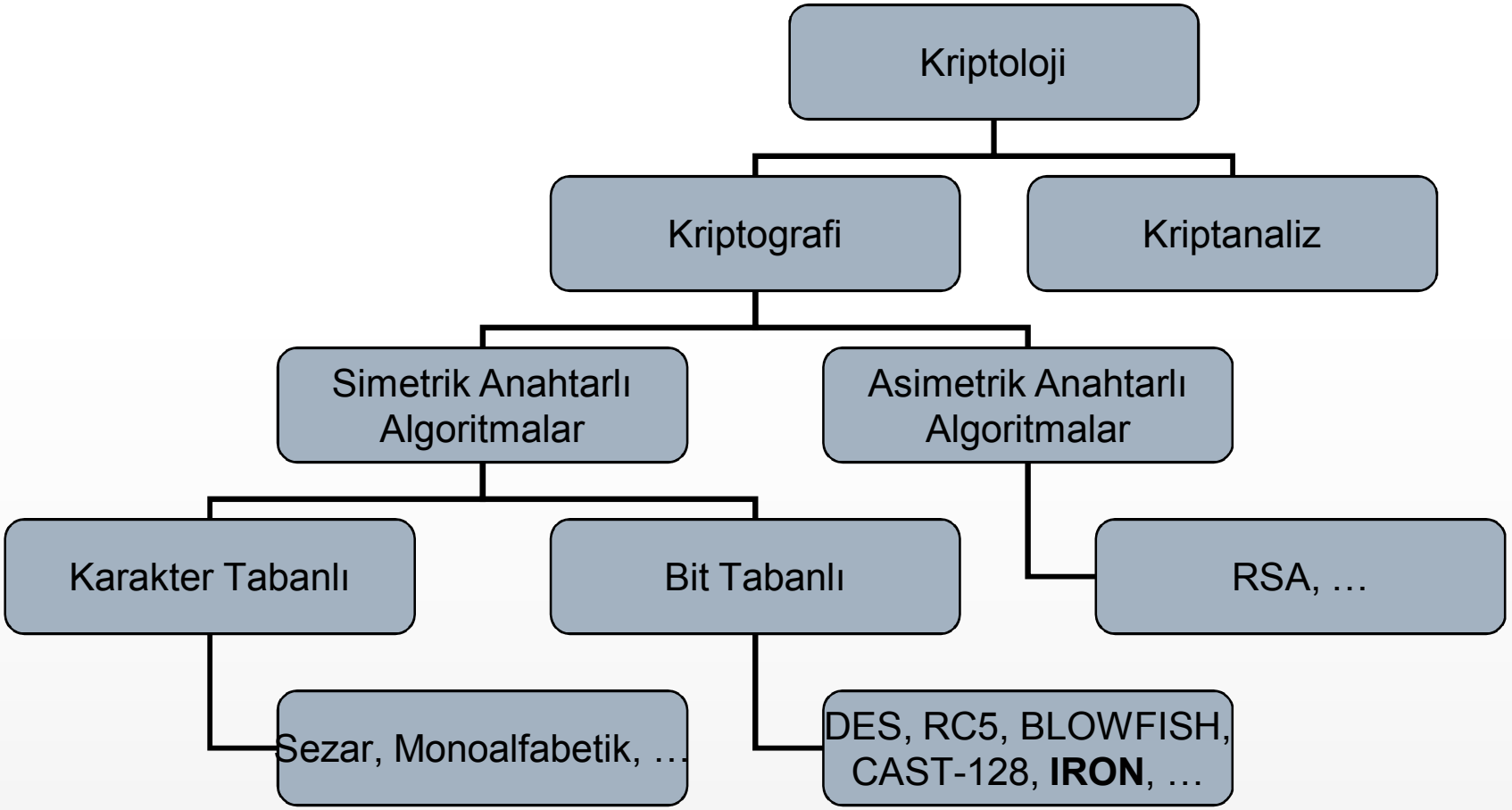
Neden Şifreleme?

- Sanal Bankacılık
- Elektronik Ticaret
- Askeri iletişim
- E-Devlet uygulamaları
- Ticari Sırlar
- Kişisel hayatın gizliliği

Bilgi Güvenliği Sorunları

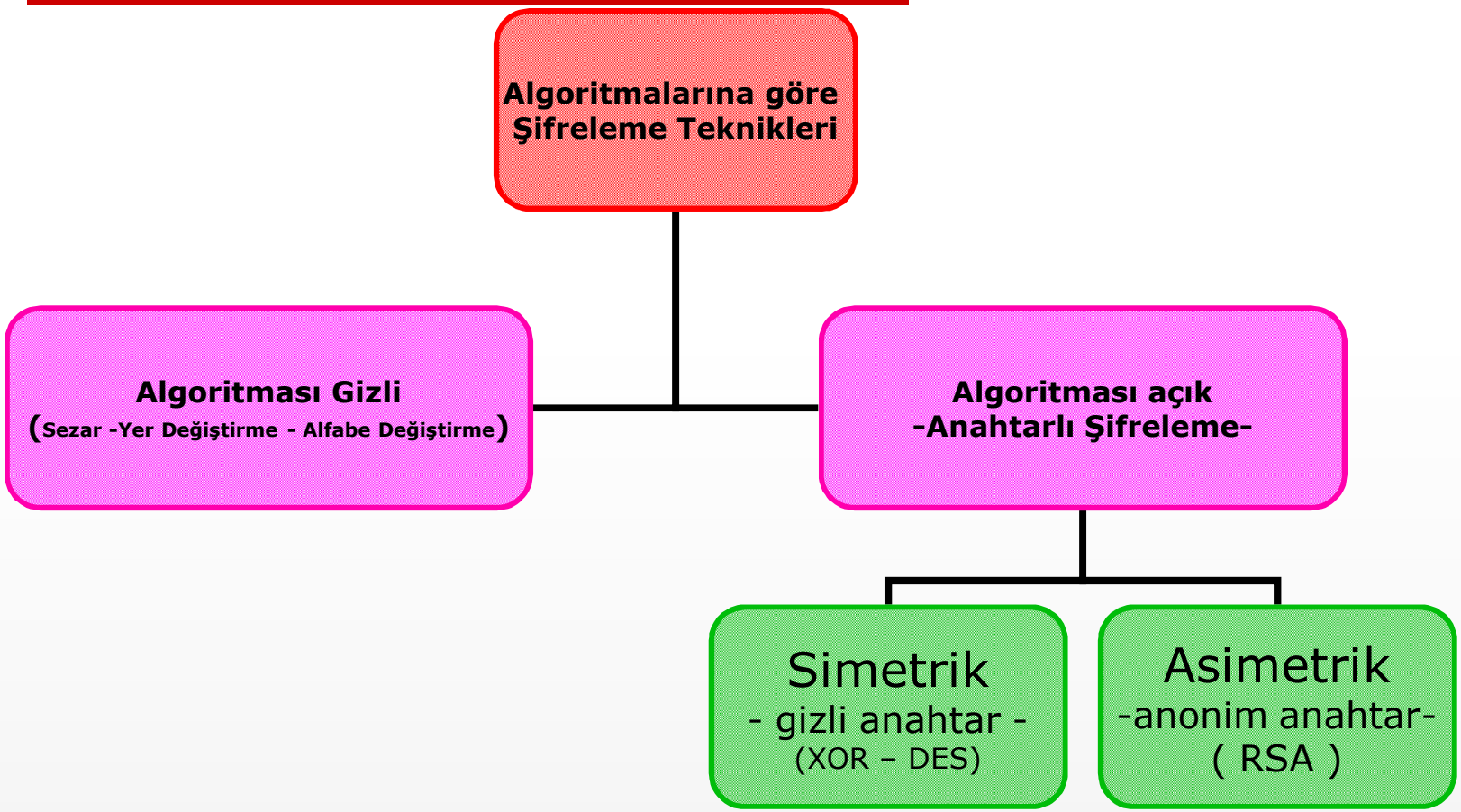
- Gizlilik,
- Bütünlük,
- İnkar Edememe

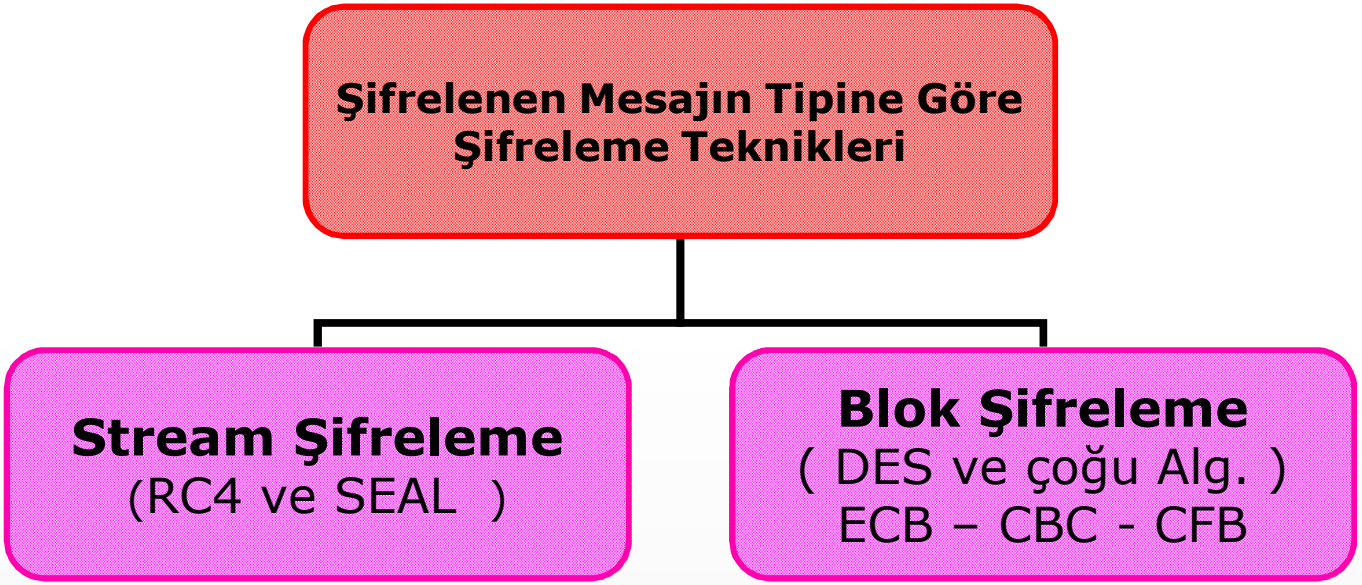
Algoritmaların Genel Tasnifi

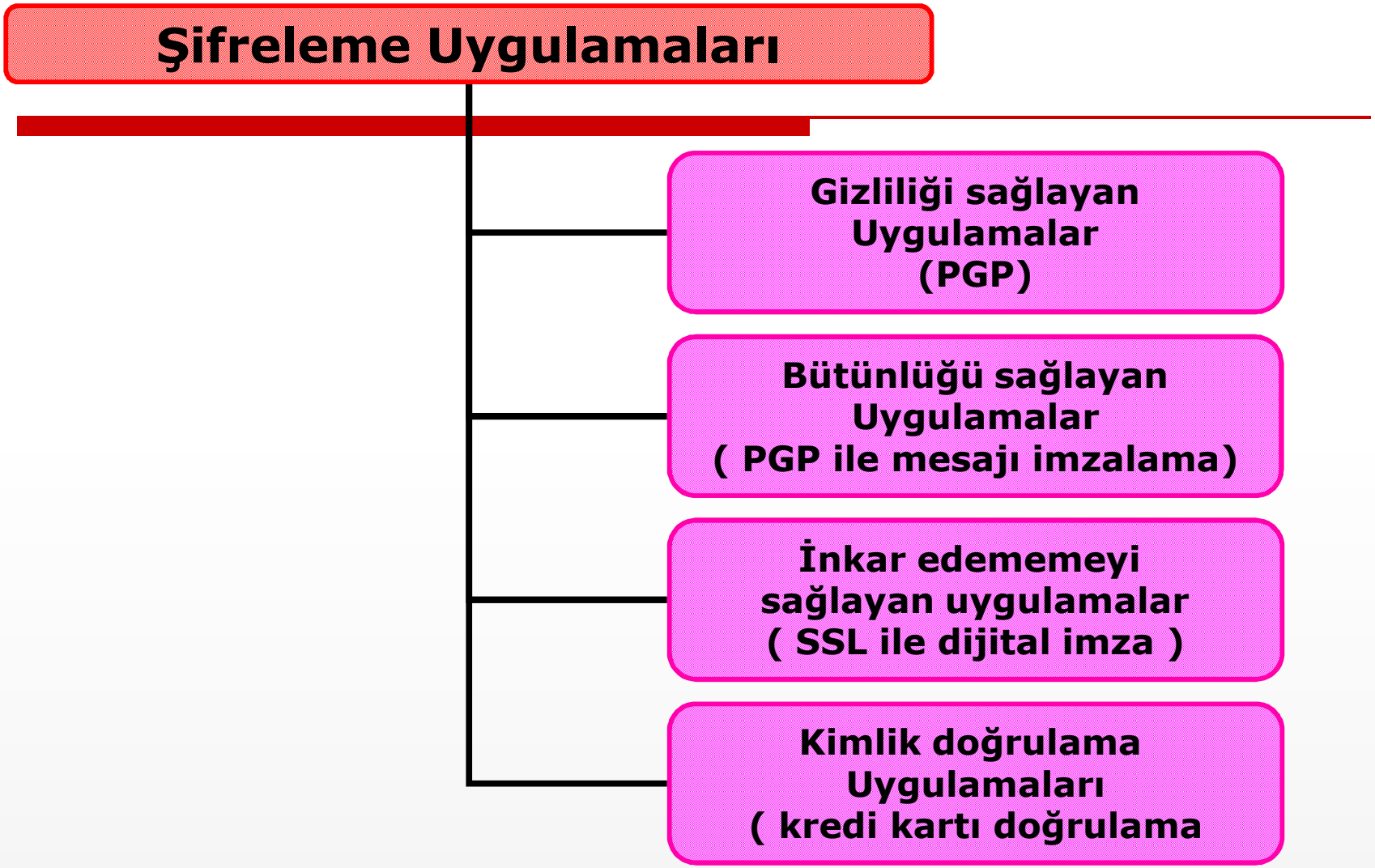


Şifreleme Algoritmalarının Sınıflandırma Kriterleri

- Algoritmanın gizliliği / açıklığı
- Anahtar Sayısı
- Şifrelenen mesajın tipi


Algoritmalarına göre
Şifreleme Teknikleri
Algoritması Gizli
(Sezar -Yer Değiştirme - Alfabe Değiştirme)
Algoritması açık
-Anahtarlı Şifreleme-
Simetrik
- gizli anahtar -
(XOR – DES)
Asimetrik
-anonim anahtar-
(RSA)


Şifrelenen Mesajın Tipine Göre Şifreleme Teknikleri
Stream Şifreleme
(RC4 ve SEAL)
Blok Şifreleme
(DES ve çoğu Alg.)
ECB – CBC - CFB


Şifreleme Uygulamaları
Gizliliği sağlayan Uygulamalar (PGP)
Bütünlüğü sağlayan Uygulamalar (PGP ile mesajı imzalama)
İnkar edememeyi sağlayan uygulamalar (SSL ile dijital imza)
Kimlik doğrulama Uygulamaları (kredi kartı doğrulama

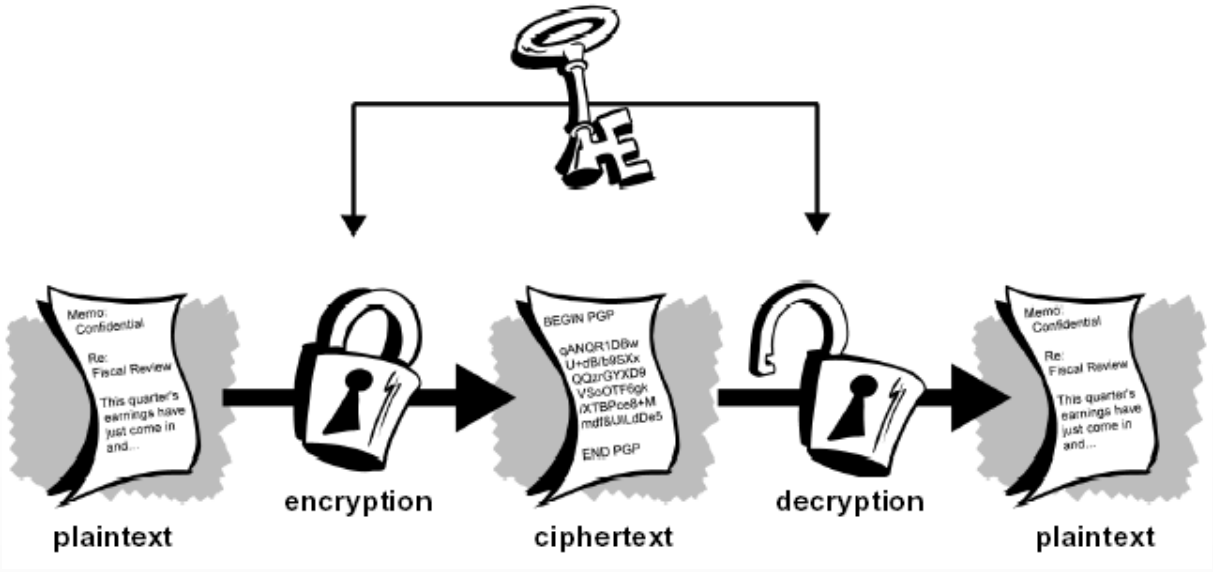
Şifreleme Algoritmalarının Performans Kriterleri

- 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.

Anahtar Uzunluğu	Sayı Değeri	10^6 şifre/s	10^9 şifre/s	10^{12}şifre/s
32 bit	~$4x10^9$	36 dak	2.16 s	2.16 ms
40 bit	~10^{12}	6 gün	9 dak	1 s
56 bit	~$7.2x10^{16}$	1142 yıl	1 yıl 2 ay	10 saat
64 bit	$1.8x10^{19}$	292 000 yıl	292 yıl	3.5 ay
128 bit	$1.7x10^{38}$	$5.4x10^{24}$ yıl	$5.4x10^{21}$ yıl	$5.4x10^{18}$ yıl

Simetrik Şifreleme Algoritmaları

- Şifreleme ve çözmede aynı anahtarı kullanma prensibine dayalı olarak çalıştıklarından "**simetrik**" olarak nitelendirilirler.
- Bu sistemlerin **avantajı** hızı, **dezavantajı** ise ortak anahtarların belirlenmesi ve taraflara iletilmesinde karşılaşılan problemlerdir.


Memo:
Confidential
Re:
Fiscal Review
This quarter's
earnings have
just come in
and...
encryption
BEGIN PGP
gANQR1DBw
U+dB/b9SXx
QQzrGYXD9
VSoOTF6gk
/XTBPce8+M
mdf8iJ/LdDe5
END PGP
decryption
Memo:
Confidential
Re:
Fiscal Review
This quarter's
earnings have
just come in
and...
plaintext
ciphertext
plaintext

Bit Tabanlı Şifreleme Sistemleri

- **1-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.

  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. Ayrıca klasik Feistel Ağı kullanılarak temelde şifreleme işleminin deşifreleme işlemiyle aynı olması sağlanmıştır. Kullanılan teknikler yayılma ve karıştırmadır. DES'in en büyük **dezavantaj**ı 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.

- **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. Standart DES'in 112 veya 168 bitlik iki veya üç anahtar ile artarda çalıştırılması ile oluşturulan bir şifreleme tekniğidir. Anahtar alanı $\mathbf{2^{112}}$ veya $\mathbf{2^{168}}$ sayısına ulaşınca bugün için veya tahmin edilebilir bir gelecekte çözülmesi **mümkün olmayan** bir kod olmaktadır

- **2-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. 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 algoritmaları**nı birbirinden farklı yapmış, bu ise uygulama maliyetini arttırmış, aynı zamanda yazılım uygulamalarını %5 yavaşlatmıştır

- **3-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 anahtarlar döngü sayısına bağlıdır. Alt anahtarların sayısı döngü sayısına eşittir. Bu nedenden dolayı **algoritma anahtar bağımlıdır**.

  IRON algoritmasının var olan algoritmalardan **farkı** da budur. Bu algoritmanın avantajı **bitler yerine 16-tabanındaki (hex) sayılar kullanmasıdır**, dezavantajı ise **yazılım için** tasarlanmış olmasıdır.

- **4-AES (The Advanced Encryption Standard) :**

  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.** Eğer bilgisayar 1 saniyede DES'i kırabilseydi, 128 bit AES anahtarı 149 trilyon yıl sonra kırılabilir.

RC4 Şifreleme

- **RC4** algoritması şifrelenecek veriyi akan bir bit dizisi olarak algılar.RC4 belirlenen anahtar ile veriyi şifreleyen bir algoritmadır. RC4'ün başlıca özellikleri şunlardır:
- 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.

MD5 Algoritması

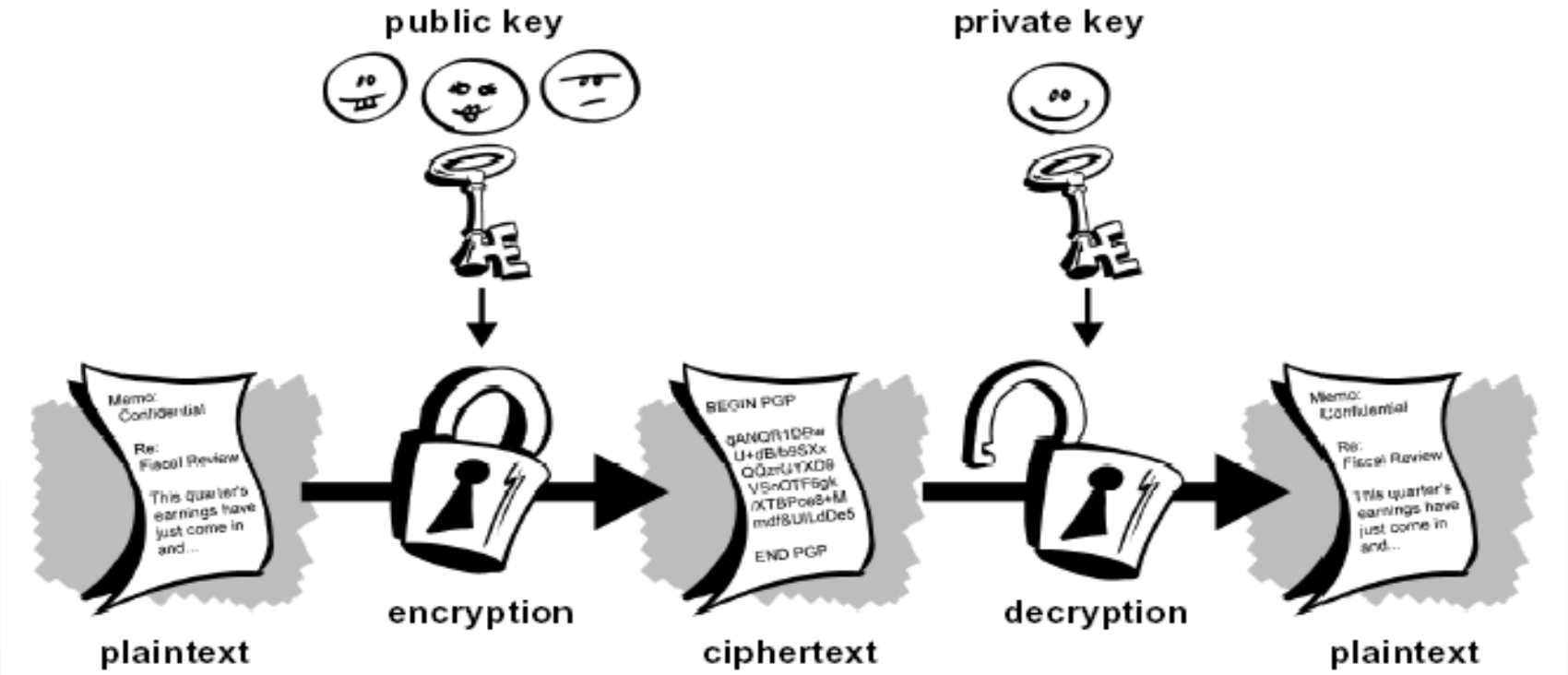
- MD5 (Message-Digest algorithm 5) Ron Rivest tarafından 1991 yılında geliştirilmiş bir tek yönlü şifreleme algoritmasıdır, veri bütünlüğünü test etmek için kullanılan, bir şifreleme algoritmasıdır. Bu algoritma girdinin büyüklüğünden bağımsız olarak 128-bit'lik bir çıktı üretir ve girdideki en ufak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

SHA AİLESİ

- 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 Şifreleme Algoritmaları

- 1976 yılında Stanford Universitesinden Diffie ve Hellman adlı araştırmacılar iki farklı anahtara dayalı şifreleme sistemi önerdiler.
- 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.


public key
private key
Memo:
Confidential
Re:
Fiscal Review
This quarter's
earnings have
just come in
and...
BEGIN PGP
qANQR1DBw
U+dB/b9SXx
QÛzrU/fXD9
VSnOTF6gk
/XTBPce8+M
mdf&UlLdDe5
END PGP
Memo:
Confidential
Re:
Fiscal Review
This quarter's
earnings have
just come in
and...
encryption
decryption
plaintext
ciphertext
plaintext

AVANTAJLARI

- 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 geliştirildi.

DEZAVANTAJLARI

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

RSA

- Dünyada en yaygın biçimde kullanılan asimetrik algoritma, ismini mucitlerinin baş harflerinden(**R**onald L.Rivest, Adi **S**hamir ve Leonard **A**dleman) almıştır.
- Büyük sayıların modular aritmetiğine dayalı çok basit bir prensibi vardır.
- Anahtarlar, iki büyük asal sayıdan üretilir. Dolayısıyla, algoritmanın güvenliği büyük sayı üretme problemine dayalıdır

Şifreleme : $y = x^e \bmod n$

Şifre Çözme : $x = y^d \bmod n$

$n = p^* q$

Şekil 4.15 RSA Şifreleme ve çözme

x : açık metin e : açık anahtar

y : şifreli metin d : gizli anahtar

n : açık modül (public modulus)

p, q : gizli asal sayılar

RSA Anahtar Elde Etme Örneği

1. İki asal sayı seç (p ve q)	p = 3, q=11
2. *Açık modülü hesapla* (public modulus)	n = p*q =33
3. Anahtar üretimi için ara bir değişken hesapla (z)	z = (p-1)*(q-1)
4. *Açık anahtar (public key) "e"* yi aşağıdaki yöntemle hesapla:	= 2*10 = 20
e < z ve gcd(z,e) = 1, yani z ve e nin en büyük ortak böleni 1. Bu özelliği sağlayan birden fazla sayı olabileceğinden biri seçilir.	e = 7
5. *Gizli anahtar "d" yi* hesapla: (d*e) mod z = 1	d = 3

RSA kullanım örneği

1. Açık metin "4" olsun	x = 4
2. Şifrele	$y = 4^7 \mod 33 = 16$
3. Şifreyi çöz	$x = 16^3 \mod 33 = 4$

RSA'da Büyük Sayı Problemi

- Smartkartın RAM'ı büyük sayıların eksponansiyelinin hesaplanması durumunda yetersiz olacağından *"modülo-üsleme"* (modulo exponentiation) denilen, ve hesaplanan değerlerin asla modülü geçmesine izin vermeyen bir yöntem kullanılır.
- Örneğin x^2 mod n değerinin hesaplanmasında yöntem çok büyük sayılarla uğraşılması gerekeceğinden (x*x) mod n işleminde biçiminde çalışmaz, bunun yerine aynı sonucu veren (((x mod n)*(x mod n)) mod n) yol tercih edilir.
- Bu daha küçük sayılarla uğraşılması demek olduğundan RSA için kullanılan bellek ve adım sayısı indirgenmiş olur.

RSA ile Kredi Kartı Şifreleme

- Public Key=79 ; Private Key=1019 olsun.
- M kart numaramız olsun ; M= 6882 3268 7966 6683,
- Önce bu sayı küçük sayılara ayrılır.
- m1=688 m2 =232 m3=687 m4=966 m5=668 m6=3
- teker teker her biri şifrelenir.
- $688^{79} \pmod{3337} = 1570 = c1$
- Aynı işlemleri diğer m_i değerleri için yaptığımızda
- C = 1570 2756 2714 2276 2423 158 değerini elde ederiz.
- Bu mesaj ağ üzerindeki terminale gönderilir. Mesajın şifre çözümü terminalde yapılır. Terminal müşterinin bilmediği gizli anahtar değerini ("d") bilir. Böylece terminal yukarıdaki mesajın şifresini çözer.
- $C1 : 1570^{1019} \pmod{3337} = 688 = m1$
- Bu yolla mesajın arta kalan kısımları geri alınabilir.

Veri Alanı Geniş Rakamlarla RSA Örneği

- p = 61 ; q = 53 (e ve d hesaplandıktan sonra bunları yokedin)
- n = p.q = 3233 <= modulus (dağıtın)
- e = 17 <= public Key (dağıtın)
- d = 2753 <= private Key (gizli tutun)
- T = Plain Text C = Chiper Text
- Encryption : encrypt(T) = (T^e) mod (n)
- = (t^17) mod 3233
- Decryption : decrypt(C) = (C^d) mod(n)
- = (C^2753) mod 3233
- Şifrelenecek Plaintext Değeri T = 123,
- encrypt(123) = (123^17) mod 3233
- = 337587917446653715596592958817679803 mod 3233
- C = 855
- Şifrelesi çözülecek Plaintext Değeri C = 855,
- decrypt(855) = (855^2753) mod 3233 =

Elde Edilen Rakam şudur.


mod 3233 = 123

Simetrik ve Asimetrik Algoritmaların Karşılaştırılması

- Simetrik algoritmalar hızlıdır fakat, ortak anahtarların güvenli bir şekilde dağıtımı problemi vardır.
- Asimetrik algoritmalar simetrik şifrelemedeki anahtar dağıtım problemini çözer fakat yavaştır.
- Bu nedenle anonim anahtarla şifreleme yöntemi birçok uygulamada gizli anahtarla şifreleme yöntemi ile birlikte kullanılır.
- Örneğin elektronik postaların şifrelenip gönderilmesinde en yaygın kullanılan yöntem hem gizli hem de anonim anahtar algoritma yöntemlerini içeren PGP programıdır.

Algoritması Bilinen Bir Şifreleme Yönteminin Gücü

- Modern Şifreleme yöntemlerinin algoritmaları dağıtılmaktadır.
- Teorik olarak, bir anahtar kullanan algoritması açık kriptografik algoritmalar, olası bütün anahtarları sırayla denemek yoluyla kırılabilir.
- Öyle ise bu algoritmaların gücü anahtar aralığı kadardır.
- Çift anahtarlı kriptografide kullanılan anahtarların uzunlukları simetrik anahtarlı kriptografide kullanılanlardan genellikle çok daha büyüktür.
- Açık anahtar algoritmayı kırabilmek için, doğru anahtarı tahmin etmek değil, açık anahtardan gizli anahtarı elde etmek gerekmektedir.

Anahtar Uzunluğu	Sayı Değeri	10^6 şifre/s	10^9 şifre/s	10^{12} şifre/s
32 bit	$\sim 4 \times 10^9$	36 dak	2.16 s	2.16 ms
40 bit	$\sim 10^{12}$	6 gün	9 dak	1 s
56 bit	$\sim 7.2 \times 10^{16}$	1142 yıl	1 yıl 2 ay	10 saat
64 bit	1.8×10^{19}	292 000 yıl	292 yıl	3.5 ay
128 bit	1.7×10^{38}	5.4×10^{24} yıl	5.4×10^{21} yıl	5.4×10^{18} yıl

Sayısal İmzalar

- Sayısal İmzalar ; kimlik doğrulama ve inkar edememeyi sağlayan bir yöntemdir.
- Ayrıca mesajların içeriğinin değişip değişmediğini sorgulamayı mümkün kılar.
- Sayısal imza doğru olarak tek bir kişi tarafından üretilir, fakat asıl imzayı bilen kişiler tarafından kontrol edilebilir.
- Bundan dolayı, sayısal imzalar için asimetrik kriptografik yöntemler uygundur.

PGP (Pretty Good Privacy)

Genel olarak PGP programı ile yapabileceklerimiz şunlardır.

- Dosya,mail ve mesajlarımızı şifreleme / çözme
- Mesajları imzalayarak şifreleme
- Anahtar oluşturma ve anahtar dağıtımı - yönetimi
- Gizli Bilgileri imha etme
- VPN ile Network trafiğini güvenli hale getirme
- Firewall ile yetkilendirilmeyen kişiler tarafından gönderilen paketleri bloke etme.

PGP Anahtar işlemleri

- **PGP kullanarak RSA anahtarları üretmek mümkündür.**
- **RSA anahtarlarının boyu kullanıcının güvenlik gereksinimine bağlı olarak 512 ile 2048 bit arasında değişebilir. O yüzden, gizli anahtarları ezberlemek ve her gerektiğinde klavyeyi kullanarak girmek nerdeyse imkansızdır.**
- **PGP'de gizli anahtarlar şifrelenerek bir dosyada saklanır ve gerektiğinde bu dosyadan okunarak işlem yapılır. Bu dosyanın adı 'secring.pgp'dir.**
- **Gizli anahtarı şifrelemek için simetrik şifreleme algoritmaları (DES, IDEA) kullanılır. . Şifreleme anahtarı 128 bit uzunluğundadır**
- **Söz konusu anahtar kullanıcının belirlediği bir şifre cümlenin (passphrase) MD5 hash algoritması kullanılarak çıkartılan özüdür.**
- **PGP, açık anahtarları 'pubring.pgp' isimli bir dosyada saklar. Açık anahtarların gizlilik gibi bir gereksinimleri olmadıkları için şifrelenmelerine de gerek yoktur.**
- **Açık anahtarlar ve üzerlerindeki imzalar, Internet üzerinden açık anahtar sunucuları vasıtasıyla istem bazında dağıtılırlar.**
- **Bir kullanıcının doğruluğuna güvenmediği bir açık anahtarı çekinmeden kullanabilmesi için ortakça tanınan ve güvenilen bir veya birkaç kişinin, ya doğrudan ya da hiyerarşik bir düzende birkaç seviyede geçişli olarak, söz konusu açık anahtarı imzalayarak kefalet vermesi gerekir.**

PGP'nin Güvenliği

- **PGP'nin güvenliği, temel olarak kullanılan Simetrik ve Asimetrik şifreleme algoritmalarının (RSA , DES, 3DES, IDEA vs.) ne kadar güvenli olduğu ile ilgilidir.**
- **Her iki algoritma da geniş çevreler tarafından yeterli anahtar uzunluğu var olduğunda güvenli olarak nitelendirilen algoritmalardır. O yüzden, PGP şifreleme bilimi açısından tamamen güvenlidir.**
- **Yine de, PGP'nin güvenliğini artırmak ve işletim sisteminin hatalarından doğabilecek güvenlik gediklerini en aza indirmek için aşağıdaki önlemleri almak gereklidir.**

PGP'nin Güvenliğini Arttıracak Önlemler

- **Gizli anahtarın güvenliğini pekiştirmek için secring.pgp dosyası bilgisayarın sabit diski üzerinde bırakılmamalıdır. Bununla beraber, gizli anahtarı şifrelemek için kullanılan şifre cümlesi mümkün olduğunca uzun (128 karakter) ve anlamsız olmalı ve hiç bir yere kaydedilmemelidir.**
- **Öte yandan, pubring.pgp dosyasının sabit disk üzerinde tutulmaması bu dosyanın yetkisiz kişilerce silinip değiştirilmesini önleyecektir.**
- **PGP şifreleri anlamsız tahmin edilemez ve sayı-karakter karışık olarak verilmelidir.**
- **Örneğin *hEllowOrld33IjustwanTtoteLLtoev3ryon3thatI'maLamErandI'mahacKer666* gibi**

- PGP'nin normal yollarla kırılamaz olduğu anlaşılmıştır.
  Fakat pass phrase güvenli seçilmeli, bilgisayarda virüs veya trojan olmadığından emin olunmalı ve PGP’nin gerçek versiyonunu kullanılmalıdır.

Kripto Analiz ve Kriptosistemlere Saldırılar

Kriptanaliz uygun anahtarların bilinmeden şifrelenmiş iletişimlerin çözülmesi işlemidir.
En önemli kriptanaliz tekniği Ortadaki adam saldırısıdır.

- iki kişi güvenli iletişim için anahtarlarını değiş-tokuş ederken, bir düşman kendisini iletişim hattındaki iki kişi arasına yerleştirir.
- Sonra bu düşman her iki kişi ile ayrı bir anahtar değiş-tokuşu gerçekleştirir.
- Her iki kişi farklı bir anahtar kullanarak işlerini tamamlayacaklardır ki bu anahtarlar düşman tarafından bilinmektedir.
- Bu noktadan sonra saldırgan uygun anahtar ile herhangi bir iletişimi deşifre edebilecek ve bunları diğer kişiye iletmek için diğer anahtar ile şifreleyecektir. Her iki tarafta güvenli bir şekilde konuştuklarını sanacaklardır, ancak gerçekte saldırgan konuşulan herşeyi duymaktadır.

Ortadaki Adam Saldırısının Engellenmesi

- Ortadaki-adam-saldırısını engellemenin bir yolu sayısal imzaları kullanabilen bir açık anahtar kriptosistemi kullanmaktır.
- Kurulum için her iki tarafta karşı tarafın açık anahtarını bilmelidir (ki bu bazen açık anahtar kriptosisteminin esas avantajını baltalamaktadır).
- Paylaşılan gizlilik oluşturulduktan sonra, taraflar kendi dijital imzalarını karşı tarafa göndermelidir.
- Ortadaki-Adam bu imzaları taklit etmeye çalışacak, fakat imzaların sahtesini yapamayacağı için başarısız olacaktır.

Brute-force saldırısıyla şifre kırmak ne kadar zaman alır?

- Eğer şifre tahmin edilemiyorsa saldırgan brute-force tekniğini kullanmaya karar verir.
- Brute-force tekniğinde işlem süresi saldırganın deneyeceği muhtemel şifrelere bağlıdır. Ve bu muhtemel şifreler, şifrelerin uzunluğu ve karmaşıklığına bağlı olarak artar.
- Muhtemel bir saldırıyı göz önüne alalım. Bir saldırgan, saniyede 15 milyon şifreyi deneyebilir. Bu mevcut olarak ulaşılabileceği iddia edilen en yüksek sayıdır. Bunu gerçekleştirebilmek için saldırganın çok hızlı bir bilgisayara sahip olması gerekir.
- Sıradaki slaytta, bu hız göz önüne alınarak şifre kırma süreleri incelenecektir. Denenen şifrelerin karmaşıklığı ve uzunluğuna bağlı olarak artan süre tabloda açıkça görülebilmektedir.

- length: 4, complexity: a-z ==> less than 1 second
- length: 4, complexity: a-zA-Z0-9 + symbols ==> 4.8 seconds
  length: 5, complexity: a-zA-Z ==> 25 seconds
- **length: 6, complexity: a-zA-Z0-9 ==> 1 hour**
- **length: 6, complexity: a-zA-Z0-9 + symbols ==> 11 hours**
- length: 7, complexity: a-zA-Z0-9 + symbols ==> 6 weeks
- **length: 8, complexity: a-zA-Z0-9 ==> 5 months**
- **length: 8, complexity: a-zA-Z0-9 + symbols ==> 10 years**
- length: 9, complexity: a-zA-Z0-9 + symbols ==> 1000 years
  length: 10, complexity: a-zA-Z0-9 ==> 1700 years
- **length: 10, complexity: a-zA-Z0-9 + symbols ➔91800 years**

- Özetlemek gerekirse, 5 karakterden daha kısa uzunluktaki bir şifre nasıl şifrelenirse şifrelensin 5 saniye içerisinde,
- 7 karakterli bir şifre bir gün içinde,
- 9 karakterli bir şifre ise yüzlerce yılda kırılabilir.
- Bu nedenle güvenli bir şifre minimum 10 karakterden oluşmalıdır. Güvenliği arttırmak için karakterler karıştırılmalıdır.

SONUÇ

- **Komplike matematiksel hesaplamalara dayalı olması sebebiyle asimetrik algoritmaların hesaplanma hızları simetrik olanlara oranla çok daha düşüktür, kaynak kullanımı ise daha fazladır. Bu sebeple uygulamada, anahtarın korunması hassasiyetinin gerekliliğine rağmen veri değiş-tokuşu miktarı fazla olmayan ve bu nedenle yüksek hız gerektirmeyen kimlik doğrulaması sürecinde asimetrik, akabinde gerçekleşecek veri akışının şifrelenmesi sürecinde ise simetrik yöntemlerin tercih edilerek kullanılmasına dayalı bir birliktelik (Ör: RSA/IDEA) mantıklı olacaktır. İki sistemin de avantajlarından yararlanmak adına asimetrik kriptosistemin güvenilirliğini ve simetrik kriptosistemin verimliliğini birleştirerek meydana getirilen modern hibrid kriptosistemler (SSL, PGP, GPG), yüklü verilerin şifrelemesini üstlenen simetrik kriptosistem anahtarlarının asimetrik algoritmalar vasıtasıyla şifrelenerek dağıtımı esasına dayanmaktadır.**