Güvenli Elektronik Belge Yönetim Sistemi İçin Temel Gereksinim: E-İMZA

Doç. Dr. Ahmet Koltuksuz

<ahmet.koltuksuz@yasar.edu.tr>

Yaşar Üniversitesi

Mühendislik Fakültesi

Bilgisayar Mühendisliği Bölümü

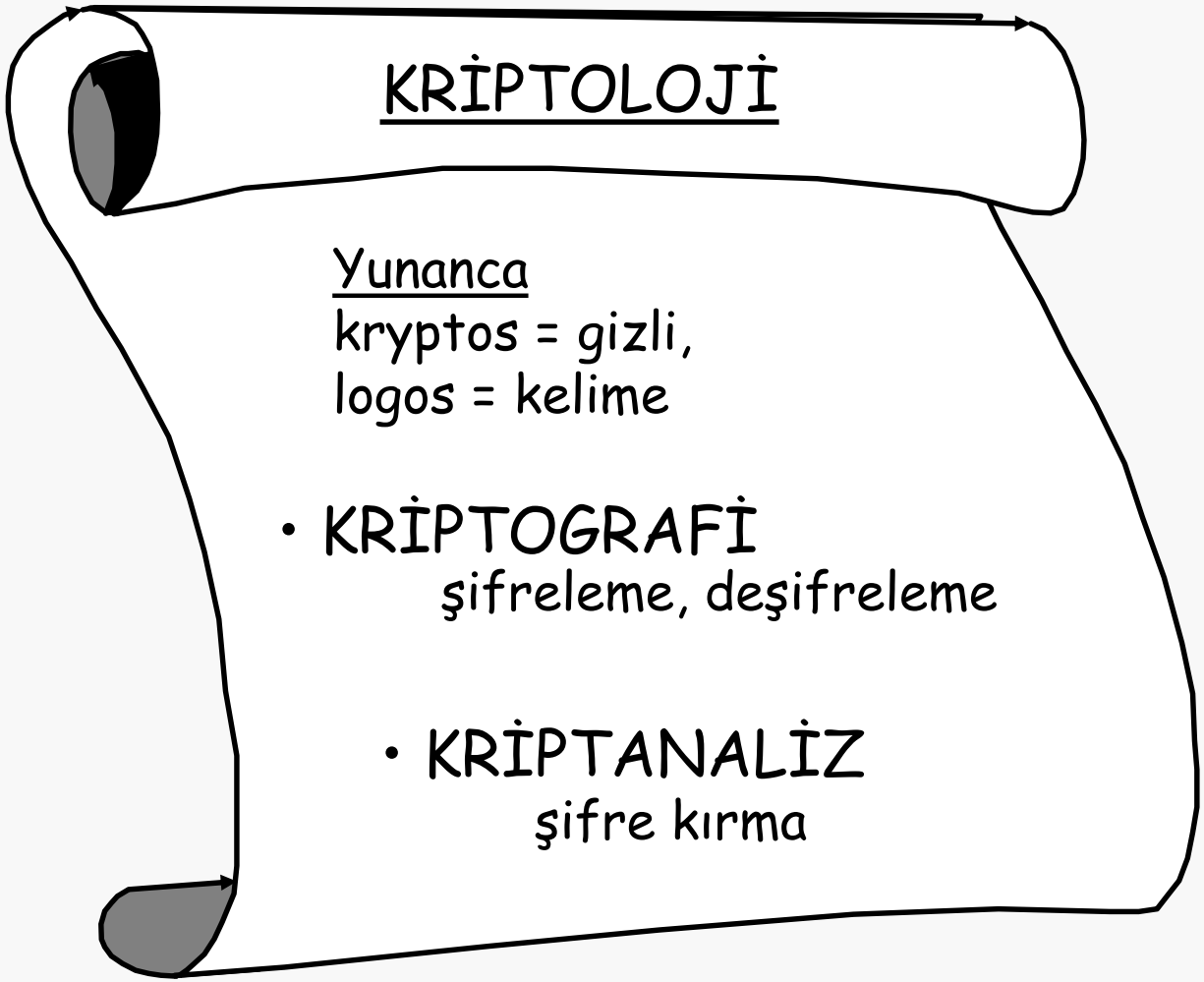
İzmir

Gündem

- Giriş
  - Tanımlar: Elektronik Belge Yönetim Sistemi, E-İmza
- Temel Kriptografi Bilgileri
  - Terminoloji, Simetrik-Asimetrik Şifreleme
- Asimetrik Kriptosistemler
- Güvenli Elektronik İşlemin Bileşenleri
  - Gizlilik, Sayısal İmza, Kimlik Denetimi
- Onay Kurumları (Nitelikli Sertifika Sağlayıcılar)
  - Adlandırma, İşlev, Tanım, Örneksemeler
  - X509 v.3 Sertifikası, Örgütlenme

Tanım

- Elektronik Belge Yönetim Sistemi, tüm evrakların elektronik biçimde tutulduğu ve bilgisayar ağ(lar)ı içinde hareket ettiği sistemdir.
- Böylesi bir sistemde bir belgenin aidiyeti de elektronik olarak sağlanır.
- Elektronik olarak sağlanan aidiyet; elektronik imza veya sayısal imza olarak bilinir.


KRİPTOLOJİ
Yunanca
kryptos = gizli,
logos = kelime
• KRİPTOGRAFİ
şifreleme, deşifreleme
• KRİPTANALİZ
şifre kırma

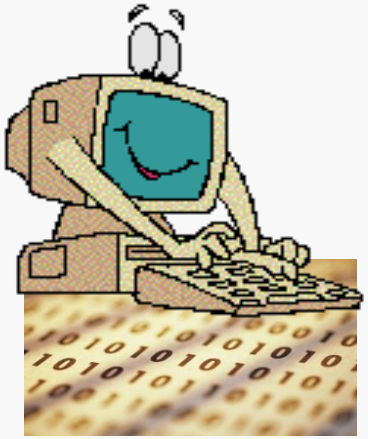
KRİPTOGRAFİK ALGORİTMALAR

	Şifreleme	Deşifreleme
	E(P) = C	D(C) = P
Anahtar (k)	$E_k(P) = C$	$D_k(C) = P$

Şimdi; $E_k = D_k$ ⇒ **Simetrik**

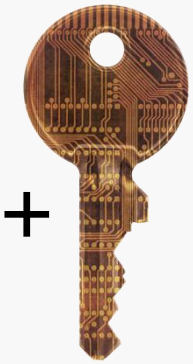
$E_k \neq D_k$ ⇒ **Asimetrik**

Simetrik=tek anahtarlı şifreleme



şifreleme programı
Ayşe

+

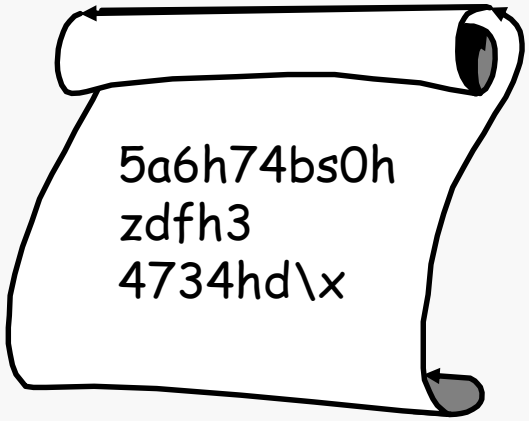


anahtar

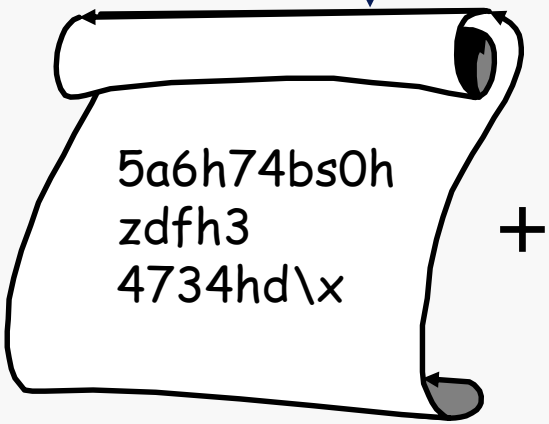
+

açık mesaj

=

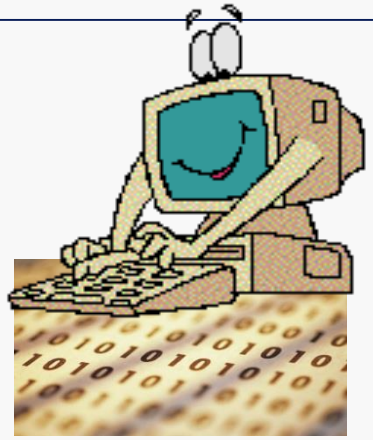


Şifrelenmiş mesaj



Şifrelenmiş mesaj

+



deşifreleme programı
Ahmet

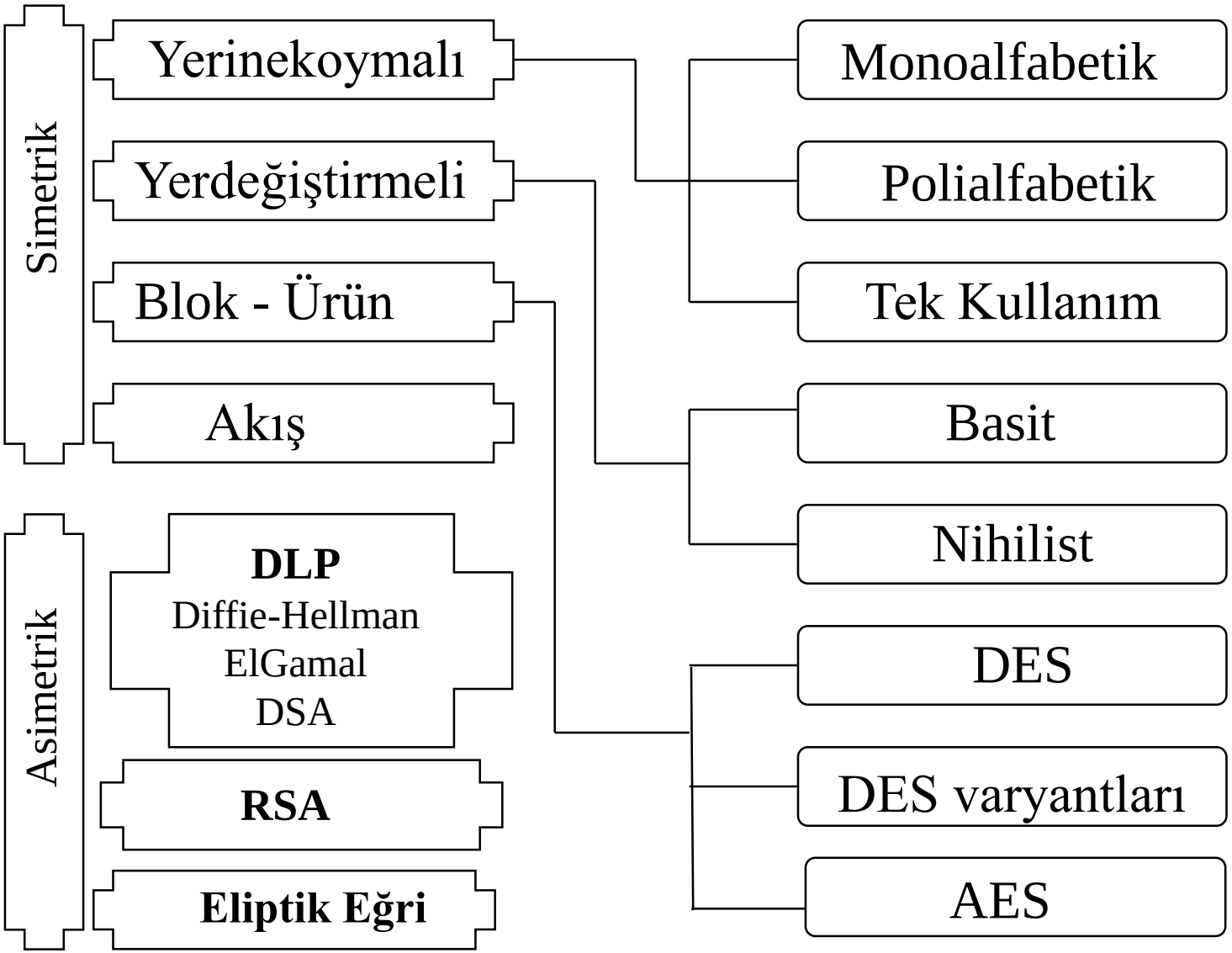
+

anahtar

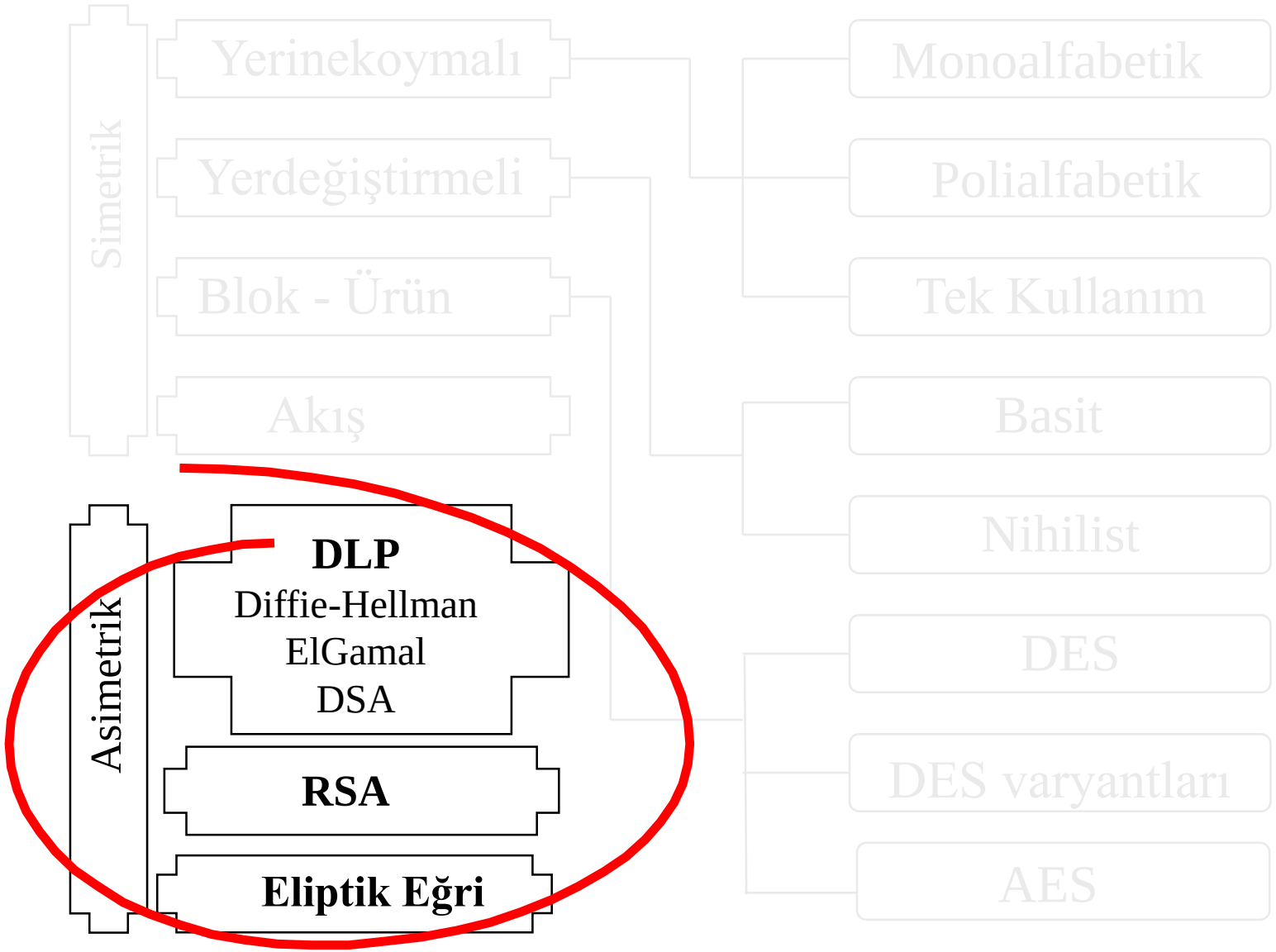
=

açık mesaj

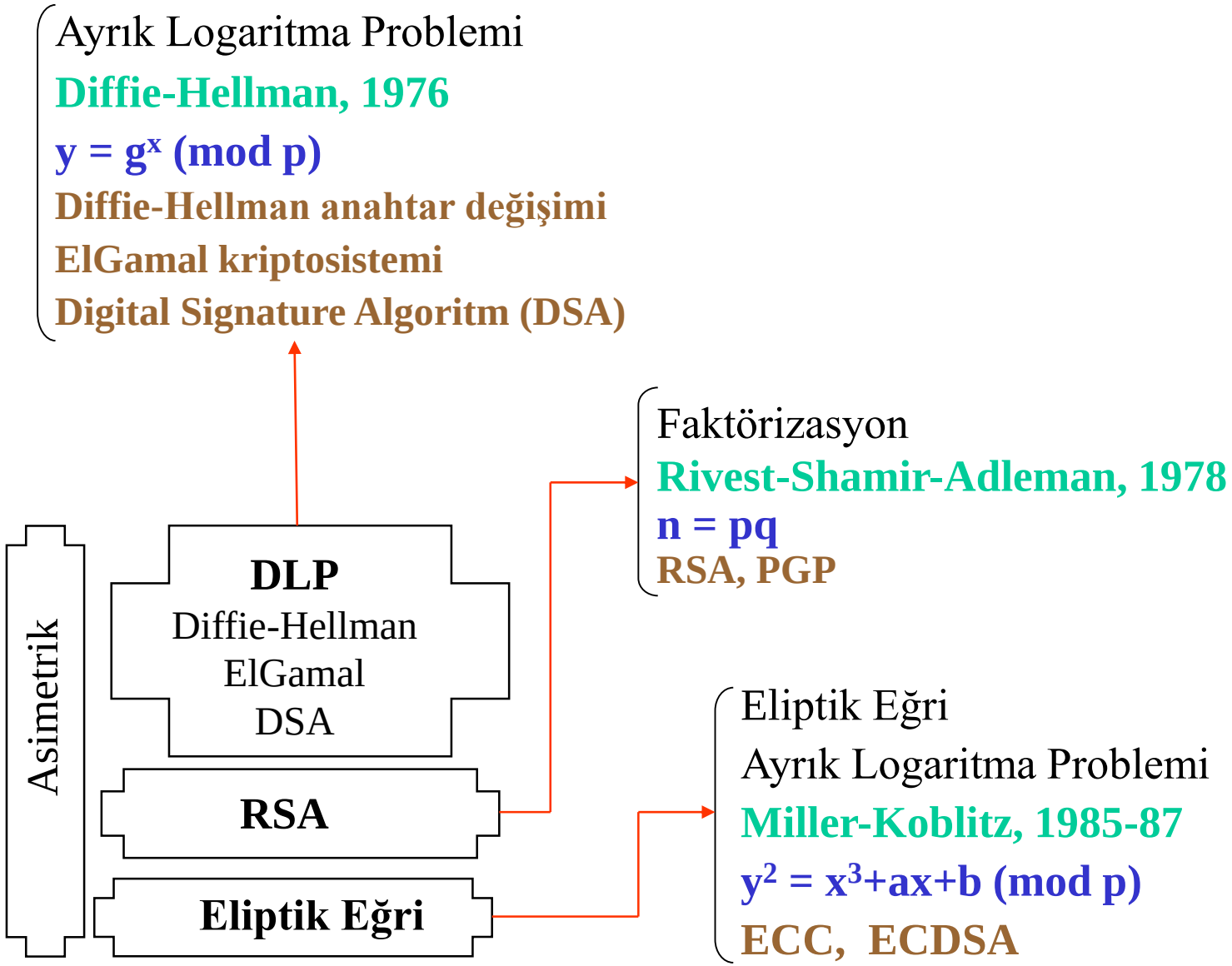
Terminoloji



Terminoloji



Terminoloji



Diffie, Hellman ve Merkle tarafından 1976 yılında ortaya atıldı.

Ana tema; iki ayrı anahtar kullanımı olup, bunlardan biri şifreleme, diğerinin deşifrelemede kullanılmasıdır.

Bir anahtardan diğerini türetmek ise çözümsüz bir sorun olmalıdır.

Alıcının şifre anahtarı, ona mesaj gönderecek herkes tarafından bilinmelidir; bu yüzden bu anahtara **AÇIK ANAHTAR** denir.

Alıcının deşifre anahtarı ise, sadece kendisi tarafından bilinir, buna da **GİZLİ ANAHTAR** denir.

Böylesi bir platform:

Açık Anahtarlı Kriptosistem

(Public Key Cryptosystem-PKC),

ve ilişkin güvenlik altyapısı ise:

Açık Anahtar Altyapısı

(Public Key Infrastructure-PKI)

olarak tanımlanır.

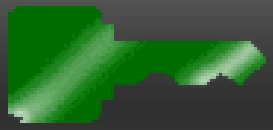
Şifre Anahtarı
[açık]

Ali : 3af56fhg465
Ayşe : hjgf89054her
Ahmet : hf723hfd984
İpek : jfsd8943jdf09
Hasan : kle*903jkegr9
Şehnaz :hjk987&()/&

Deşifre Anahtarı
[gizli]

Ali : bfh467rıu%+
Ayşe : /&'^Grtwe35
Ahmet : H+^!jklşreıre
İpek : ÜĞ??=e87djk
Hasan : _?()Kyh78sd3
Şehnaz:)hjF'!/%h&36

Şifre Anahtarı
[açık]

Ali : 3af56fhg465
Ayşe : hjgf89054her
Ahmet : 

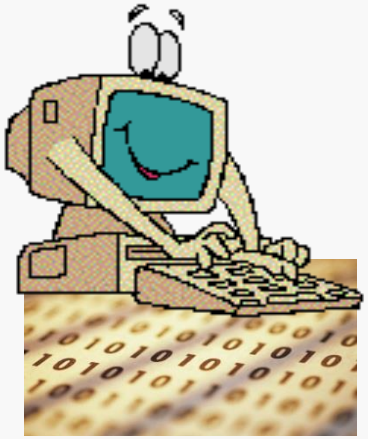
İpek : jfsd8943jdf09
Hasan : kle*903jkegr9
Şehnaz :hjk987&()/&

Deşifre Anahtarı
[gizli]

Ali : bfh467rıu%+
Ayşe : /&'^Grtwe35
Ahmet : 

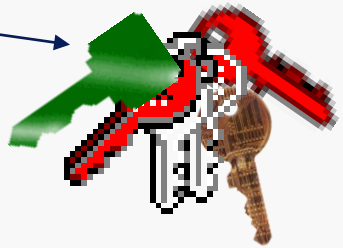
İpek : ÜĞ??=e87djk
Hasan : _?()Kyh78sd3
Şehnaz:)hjF'!/%h&36

Asimetrik=çift anahtarlı şifreleme



şifreleme programı
Ayşe

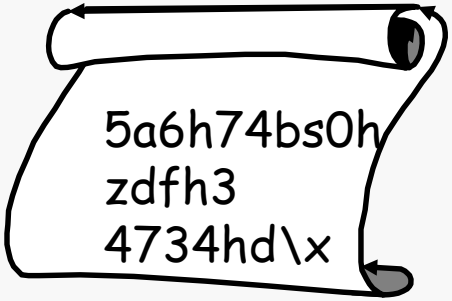
Ahmet'in açık anahtarı



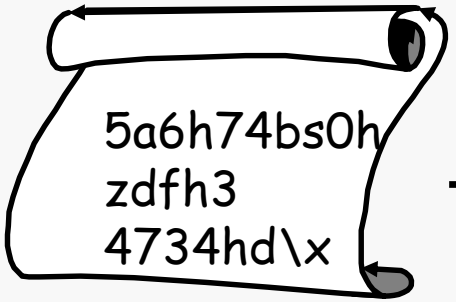
\+

açık mesaj

=

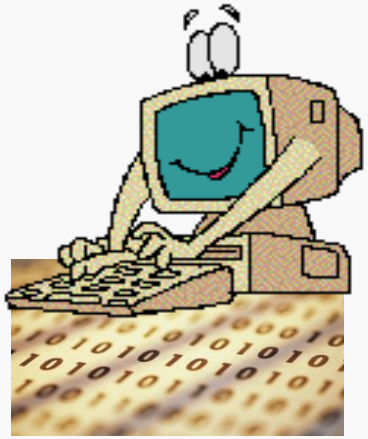


Şifrelenmiş mesaj



Şifrelenmiş mesaj

\+



deşifreleme programı
Ahmet

\+

Ahmet'in gizli anahtarı

=

açık mesaj

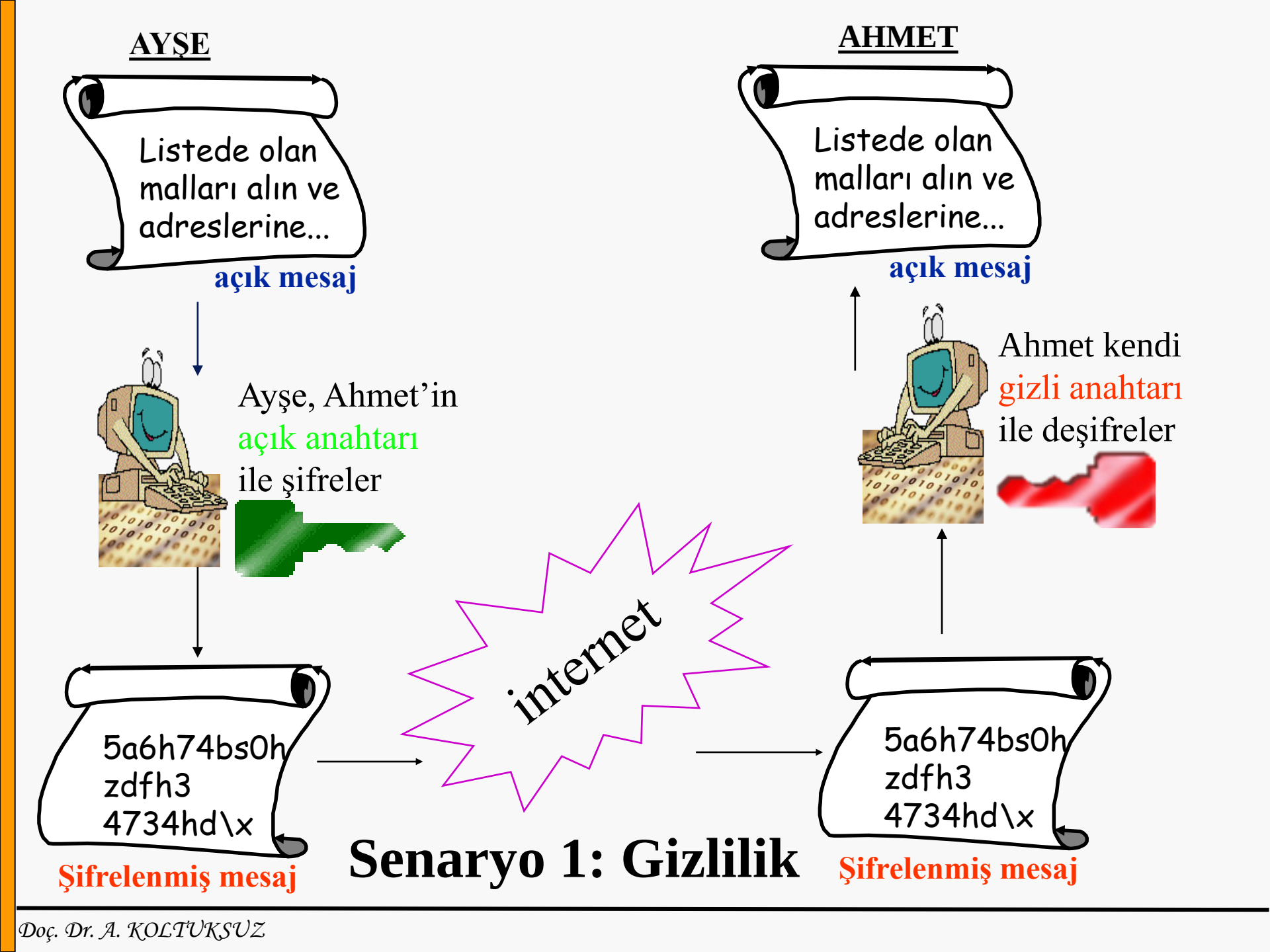
Güvenli Elektronik İşlemin Bileşenleri

1. Gizlilik
2. Doğruluk-Bütünlük: Aidiyet-Sayısal İmza
3. Kimlik Denetimi ve İnkar Edilemezlik

} ASİMETRİK KRİPTOSİSTEM UYGULAMALARI (çift anahtarlı)

A. Erişim Denetimi
B. Hizmetin Sürekli Var Olması
C. İnternet Güvenliği

} BİLGİSAYAR GÜVENLİĞİNİN DİĞER ALANLARI


AYŞE
Listede olan malları alın ve adreslerine...
açık mesaj
Ayşe, Ahmet'in açık anahtarı ile şifreler
5a6h74bs0h zdfh3 4734hd\x
Şifrelenmiş mesaj
internet
AHMET
Listede olan malları alın ve adreslerine...
açık mesaj
Ahmet kendi gizli anahtarı ile deşifreler
5a6h74bs0h zdfh3 4734hd\x
Şifrelenmiş mesaj
Senaryo 1: Gizlilik

İmzanın Tanımı

İmza, kişinin kendisi tarafından, bir yazılı belge içeriğinin o kişiye ait olduğunu göstermesi amacıyla, belgeye o kişinin adının yazılmasıdır.

İmzanın Özellikleri

Her imza;

- özgün,
- sahtesi yapılamayacak,
- tekrar kullanılamayacak,
- değiştirilemeyecek ve
- reddedilemeyecek

bir şekilde atılmalıdır.

İşte imzanın bu özelliklerini **sayısal** olarak yapmanın yolları…

Ya da kısaca, kriptografi uygulamaları = **e_imza**

H=h(m)

h : Hash fonksiyonu,

m : Değişken uzunlukta mesaj,

H : Mesajın sabit uzunluktaki hash değeri.

H=h(m)

Hash değeri aynı zamanda :

- Mesaj Özü (message digest),
- Parmak İzi (fingerprint) veya
- Sayısal Parmak İzi (digital fingerprint)

olarak da bilinir.

H=h(m)

- SHA-1 (Secure Hash Algorithm-1) ABD Standartlar ve Teknoloji Milli Enstitüsü (NIST) tarafından, 17.4.1995 tarihinde, FIPS PUB 180-1 numaralı standart olarak ilan edildi.
- 1 Ağustos 2002 tarihinde FIPS PUB 180-2 standardı, SHA-1, SHA-256, SHA-384 ve SHA-512 olmak üzere 4 ayrı tipi ortaya koydu. Sırasıyla, 160, 256, 384 ve 512 bitlik H değeri üretmektedir
- **1.1.2014'den itibaren SHA3-Ketchak algoritması kullanıma girdi.**

H=h(m)

- MD5-SHA0 (160 bits)-SHA1 (256 bits) algoritmaları kırıldı. Bu nedenle kullanılmamaları gerekir.
- Kullanılması gereken ise SHA3 ailesidir.

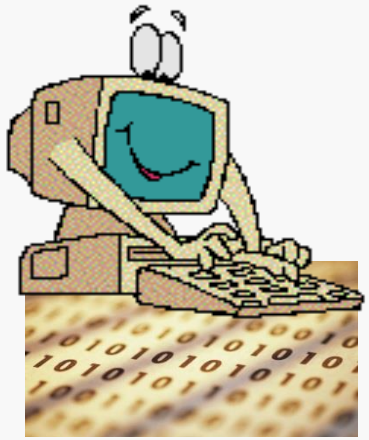
- ✓ Wang, X., Feng, D., Lai, X., Yu, H., ”Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD”, Cryptology ePrint Archive, Report no: 2004/199, 2004.
- ✓ Wang, X., Yu, H., Yin, Y. L.,”Efficient Collision Search Attacks on SHA-0.”, Springer,Lecture Notes in Computer Science, v.3621, pp.1-16, 2005.
- ✓ Wang, X., Yin, Y.L., Yu, H., “Finding Collisions in the Full SHA-1”, Springer,Lecture Notes in Computer Science, v.3621, pp.17-36, 2005.

Hash Fonksiyonlarına örnekler…

Sayısal İmza

Listede olan malları alın ve adreslerine...

açık mesaj



Hash fonksiyonu

Secure Hash Algorithm (SHA)

Hash Değeri

we09854jkl
)/(&hj37894

160 bit

Ayşe, kendi
gizli anahtarı
ile hash değerini şifreler

+

Hash Değeri

we09854jkl
)/(&hj37894

=

SAYISAL İMZA

Ayşe

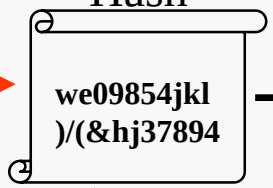
AYŞE

Senaryo 2: Doğruluk/Bütünlük-Sayısal İmza

1)

açık mesaj

→ Hash



Ayşe

+

Ayşe, kendi
gizli anahtarı
ile hash değerini şifreler

=

Ayşe

2)

açık mesaj

+

Ayşe

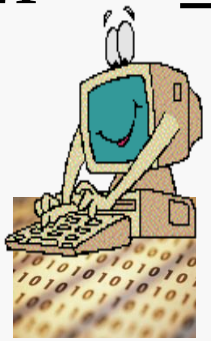
→

Ayşe, Ahmet'in
açık anahtarı
ile şifreler

→ internet →

AHMET

Senaryo 2: Doğruluk/Bütünlük-Sayısal İmza

1) 

Ahmet kendi gizli anahtarı ile deşifreler

=

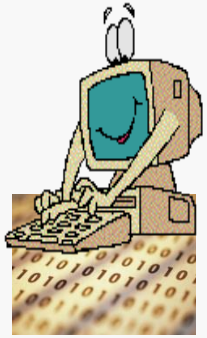
SAYISAL İMZA

Ayşe

+

Listede olan malları alın ve adreslerine...

açık mesaj

2) 

Ahmet, Ayşe'nin açık anahtarı'nı kullanarak

+

SAYISAL İMZA

Ayşe

=

Hash

we09854jkl
)/(&hj37894

Ayşe

3) 

Hash programı

+

Listede olan malları alın ve adreslerine...

açık mesaj

=

Hash

we09854jkl
)/(&hj37894

Ahmet

4)

Hash

we09854jkl
)/(&hj37894

Ahmet

?=

Hash

we09854jkl
)/(&hj37894

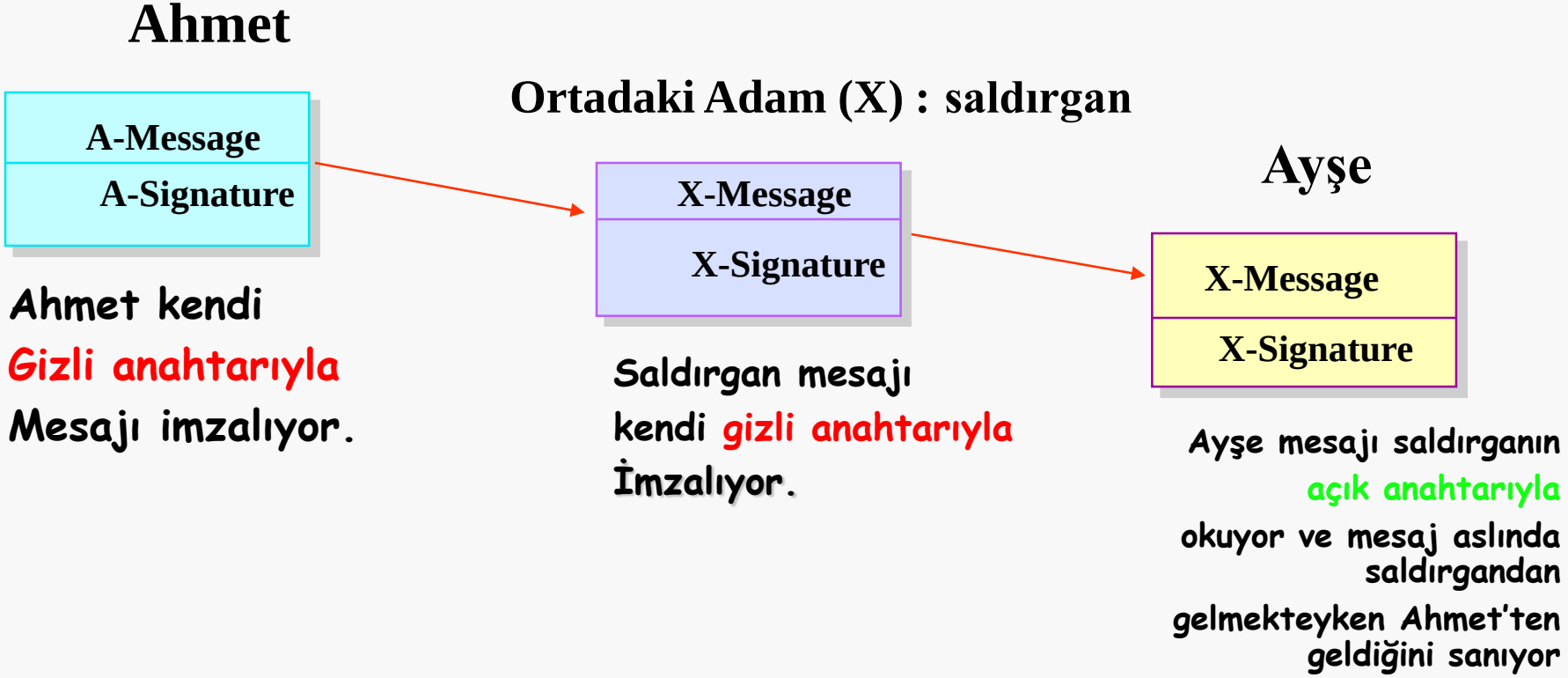
Ayşe

EVET: İşlem tamam

HAYIR: İptal

Zincir en zayıf halkası kadar güçlüdür…

Ortadaki Adam Saldırısı (Man-in-the-Middle Attack)



Gereksinim: Ahmet'in açık anahtarıyla Ahmet'in kimliği arasında;

Ayşe'nin tam olarak güvenebileceği bir bağ (=sertifika) oluşturmak

Adlandırma

- Güven Merkezi (Trust Center)
- Güvenilen Üçüncü Kurum (Trusted Third Party)
- Onay Kurumu (Certification Authority)

Veya 5070 sayılı e-imza kanununda yer aldığı gibi:

Nitelikli Sertifika Sağlayıcı

olarak da bilinir.

İşlev

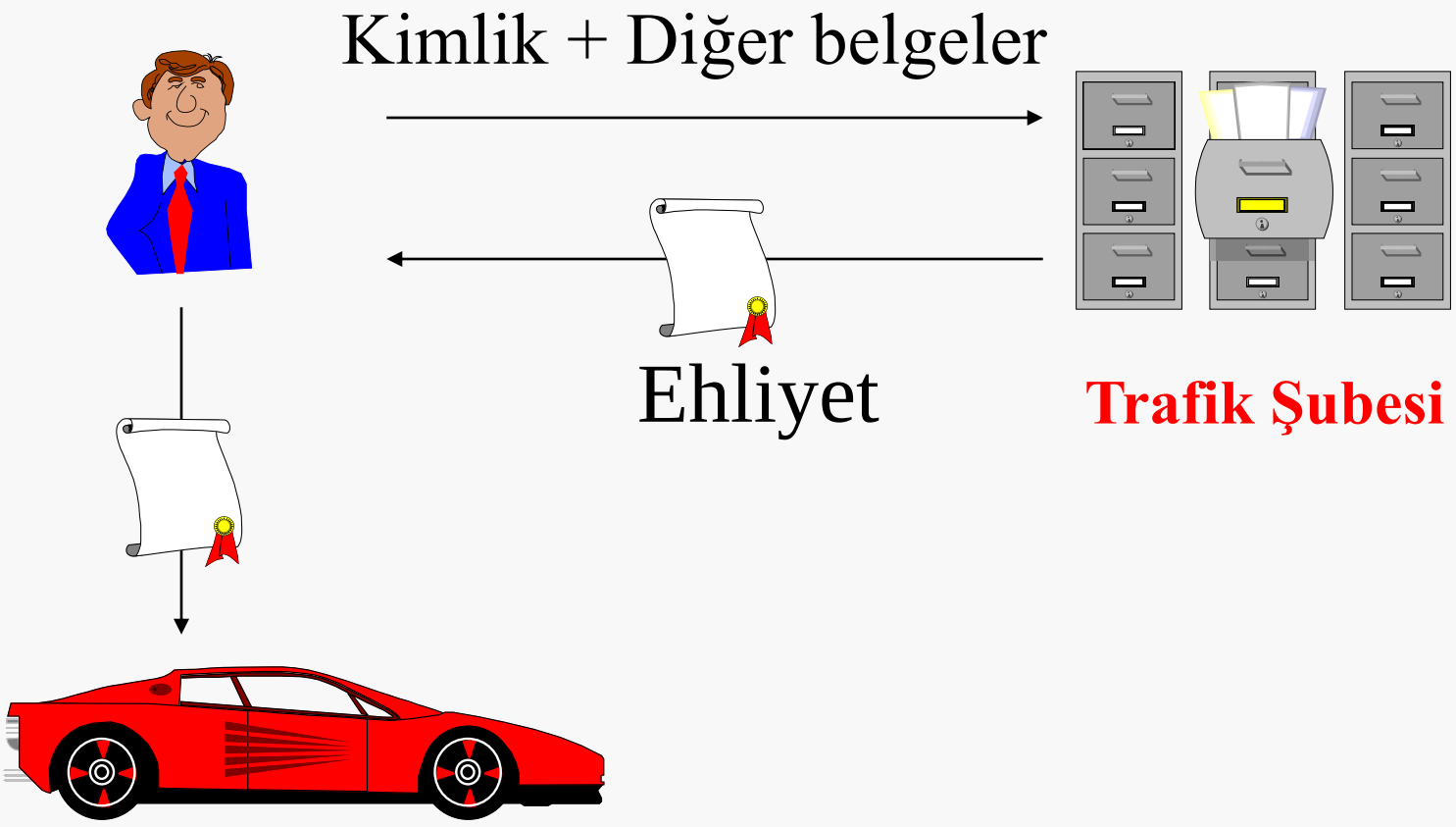
- Açık Anahtarlı Kriptosistem ile kullanılır.
- Kullanıcılara Nitelikli Güvenlik Sertifikaları sunar.

Onay Kurumu (Nitelikli Sertifika Sağlayıcı):Tanım

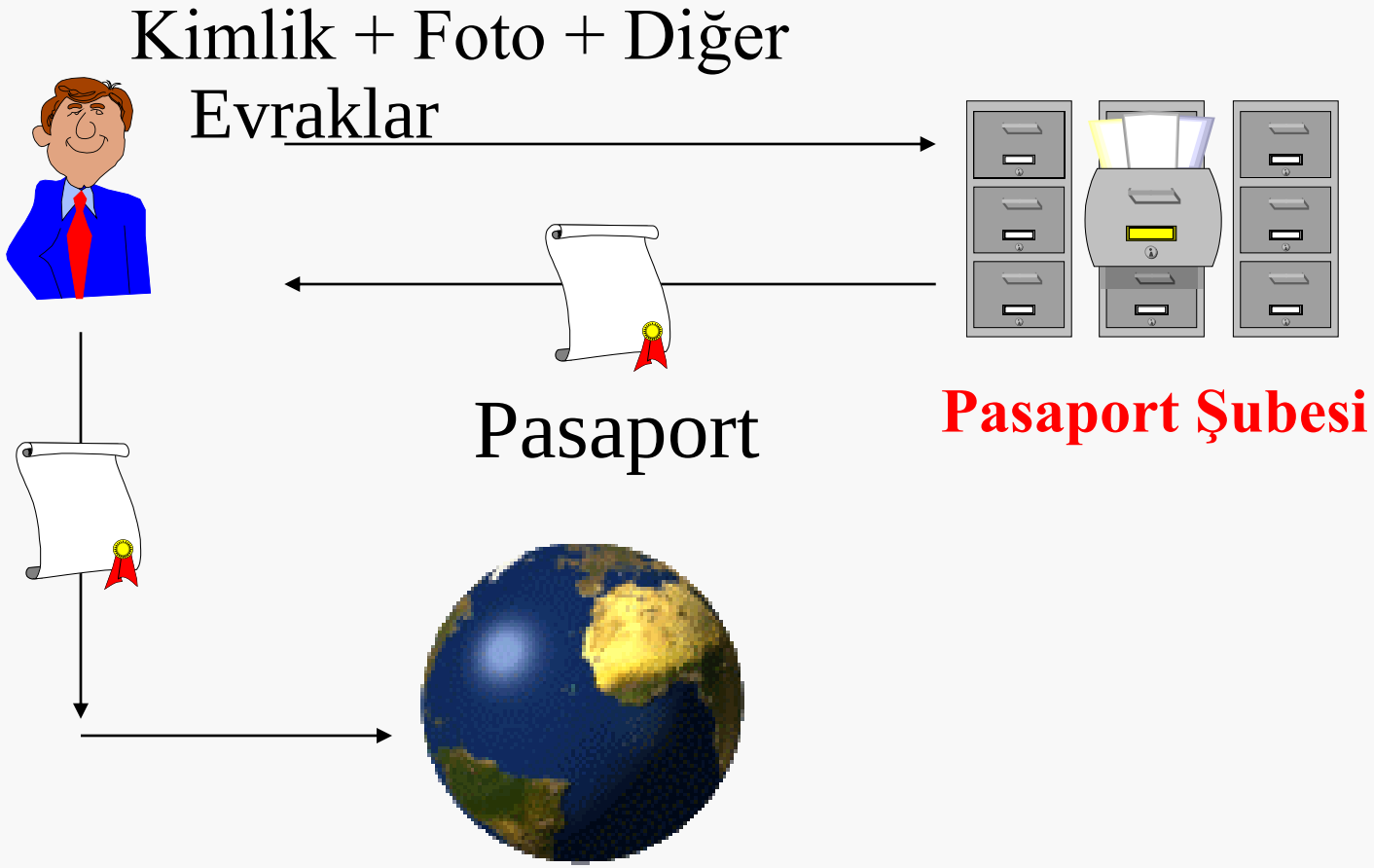
- Kişilere ait Açık Anahtarlarla, bu kişilerin gerçek kimlikleri arasında;
- hiç bir tereddüt ve şüpheye yer bırakmayacak şekilde bağ kuran,
- bu bağı nitelikli bir sertifika ile belgeleyen,
- isteyen tüm gerçek ve tüzel kişilere sertifikayı sunan,
- sertifikasyon ile ilgili
  - ❖ Saklama,
  - ❖ iptal etme ve
  - ❖ Güncelleme

gibi diğer tüm işlemleri de güvenli ve güvenilir biçimde yapan kurum (Koltuksuz, 1998).

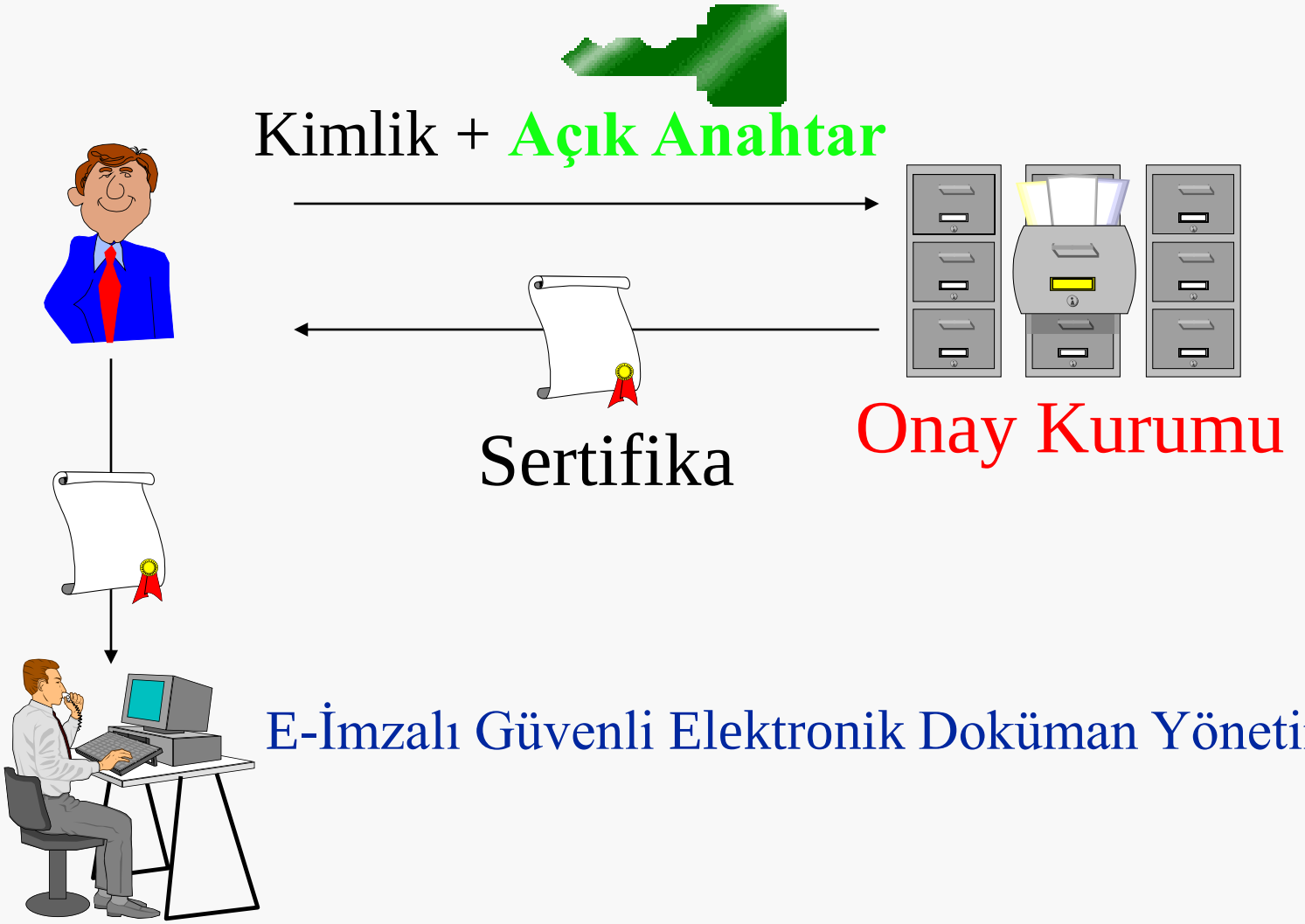
Örnekseme - 1



Örnekseme - 1



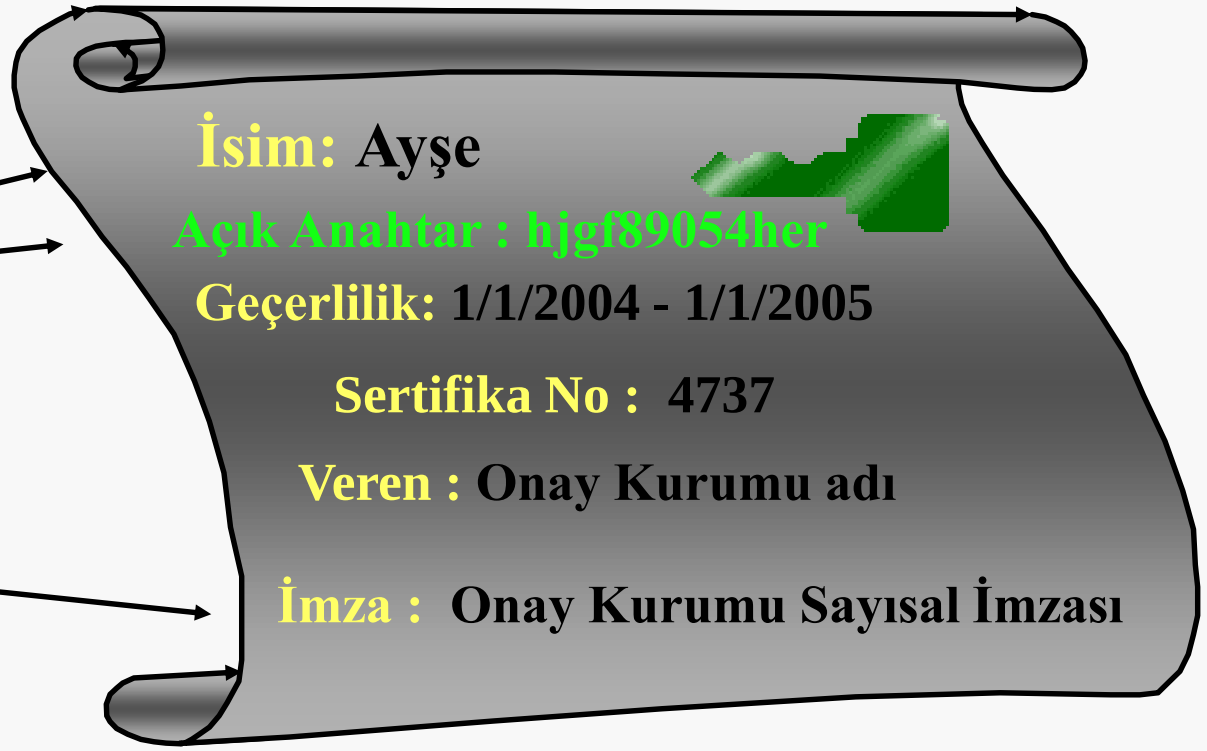
Onay Kurumları



Sertifikasyon…
Evet ama, NASIL ?

Sertifika, kişi ile açık anahtarını güvenli ve güvenilir biçimde birbirine bağlar.

Onay Kurumu imzası, sertifikanın özgün olduğunu gösterir.



Sertifikalar disk, akıllı kart, flash bellek gibi ortamlarda saklanabilir.

ITU
X.509 v.3 Sertifikası

Sertifikasyon…
Evet ama, Nereden?

E-Güven
Türk Trust
E-Tuğra

İlgi ve zamanınıza çok teşekkür ederim.