The Asymmetrical Protocols

Ahmet Koltuksuz, Ph.D., Assoc. Prof.

<ahmet.koltuksuz@yasar.edu.tr>

Yasar University

College of Engineering

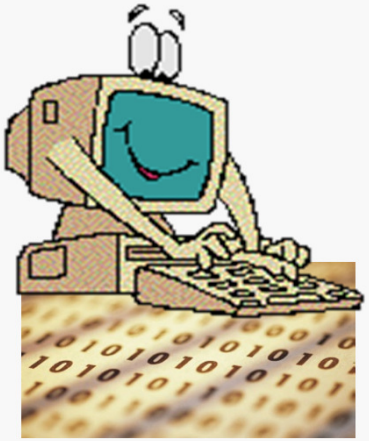
Department of Computer Engineering

İzmir, Turkey

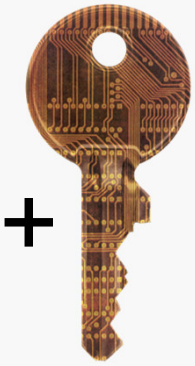
AGENDA

1. Symmetrical & Asymmetrical protocols
2. PKC-PKI
3. E-commerce security primitives
4. Secrecy
5. Integrity: Hash functions & digital signatures
6. Certification Authorities & X509 v.3
7. Authentication

Symmetrical= secret (single) key



Encryption
Alice



key

Buy the items
and send them
to the...

plaintext

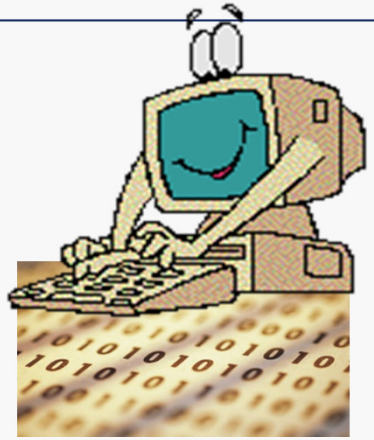
=

5a6h74bs0h
zdfh3
4734hd\x

ciphertext

5a6h74bs0h
zdfh3
4734hd\x

ciphertext



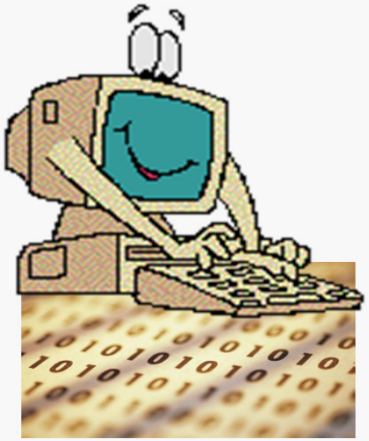
Decryption
Bob

key

Buy the items
and send them
to the...

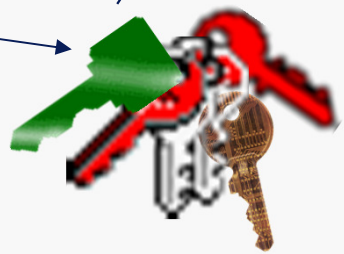
plaintext

Asymmetrical=private (secret) & public key



Encryption
Alice

Bob's public key



\+

Buy the items and send them...

plaintext

=

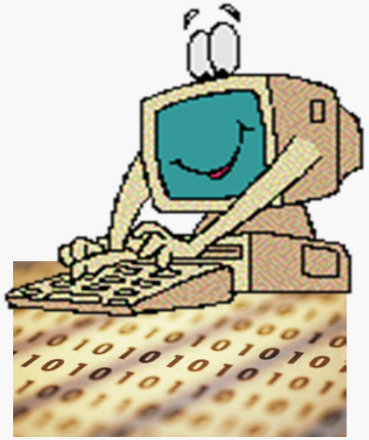
5a6h74bs0h
zdfh3
4734hd\x

ciphertext

5a6h74bs0h
zdfh3
4734hd\x

ciphertext

\+



Decryption
Bob

\+

Bob's Private key

=

Buy the items and send them...

plaintext

- The idea was belong to Diffie & Hellman plus Merkle.
- The essence is that the keys should come in pairs, one for encryption and one for decryption.
- It should not be feasible (intractable) to generate one key from the other.

- Receiver's encryption key is known and utilised by all who want to send a message to him/her, hence the term:

PUBLIC KEY.

- While the decryption key is only known by the legitimate receiver, hence the term:

PRIVATE (SECRET) KEY.

- So, the whole system is known as the Public Key Cryptosystem (PKC),

and the related infrastructure as the

- Public Key Infrastructure (PKI).

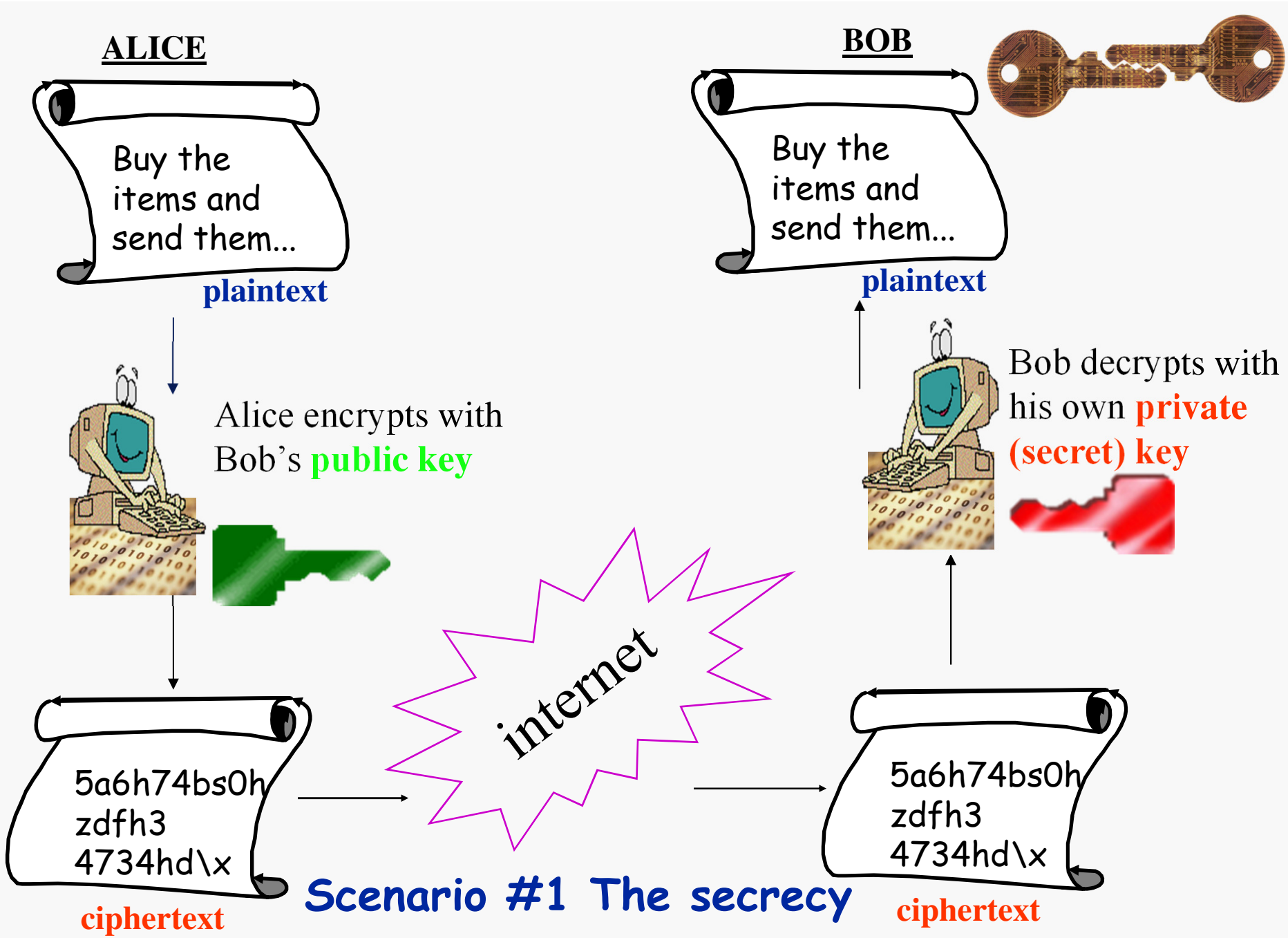
Components of a secure e-commerce

1. Secrecy
2. Integrity: Digital Signature
3. Authenticity

} ASYMMETRICAL CRYPTOSYSTEMS

- Access control
- Non-repudiation
- Availability

} The other fields of computer security


ALICE
Buy the items and send them...
plaintext
Alice encrypts with Bob's public key
5a6h74bs0h zdfh3 4734hd\x
ciphertext
internet
BOB
Buy the items and send them...
plaintext
Bob decrypts with his own private (secret) key
5a6h74bs0h zdfh3 4734hd\x
ciphertext
Scenario #1 The secrecy

- ## Definition of the Signature

A signature is a person's name written by him(her)self as a proof of authorship of the contents of a document.

- ## Peculiarities of the Signature

The signature should be authentic, unforgeable, not reusable, and of be unalterable plus should not be repudiated.

- And, this is how one can obtain the same characteristics digitally !!!

A hash function of *h* is given as H=h(m), where

h : Hash function,

m : variable length message,

H : fixed length hash value of the message.

Also known as:

- The message digest,
- The fingerprint or,
- The digital fingerprint of the message.

$H=h(m)$

- The hash value (H) should be calculated relatively easily for any given message (m).
- h(m) should be a one-way function (computationally intractable).
- There should be only one H value for any given m (collision free).

$H=h(m)$

- SHA-1 (Secure Hash Algorithm-1) was announced as a standard hashing algorithm FIPS PUB 180-1 by National Institute for Standards and Technology (NIST) of USA in 17.4.1995 and it produced 160 bit H value.
- NIST announced FIPS PUB 180-2 in August 1 2002. With this update, SHA-256, SHA-384 & SHA-512 surfaced.
- H values from SHA family are 160, 256, 384 & 512 bits respectively, in FIPS PUB 180-2.

$H=h(m)$

HashCalc

Data Format: Text string

Data: 1234567890***a string for a test of hash functions****0987654321

HMAC

Key Format: Text string

Key: 1234567890***a string for a test of hash functions****0987654321

MD5	d409cc25ab04c8a05621be8abeafad1b
MD4	aa1ff2793d0465b3ece4a710abb62a26
SHA1	18d5194885ac1afe68c455d2133d2d570e4a577f
SHA256	22f877736e3f83ff296c5be1078778beb530e2ee9ee968cbd741dd80c92108e6
SHA384	7fc67df9d6e958f0314f7744bd84c8a7c9cc0ec7be5ea1acf983f553680e34823ed137cae4fce28109ea0daef2a2cbc3
SHA512	767ce8c662258057a4768f114038690631d1b6d428b7e6131f6562317ecbc996fa27c0d0f5b93c258c2305d5f4245f4ac99c98526b62539232e735c34b74562e
RIPEMD160	34158b0d94cbef25e6ff7e664f9ace997035461f
PANAMA	5a378dbeb79b955af040416e75f0613e35dde5959fb70f5343a7c706a4d8b5af
TIGER	08abfe9fdafec7b6b3482375df85f24e0360324e5ded8a9a
MD2	4117f975c9ef250f04258583c3bd9281
ADLER32	607d12d3
CRC32	bd7f185b
eDonkey/ eMule	aa1ff2793d0465b3ece4a710abb62a26

SlavaSoft

Calculate Close Help

Some hash values for different hash functions.

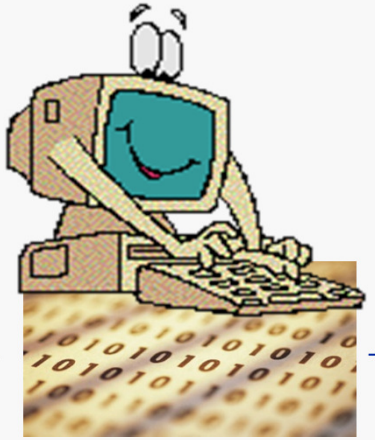
- MD5-SHA0 (160 bits)-SHA1 (256 bits) have already been broken thus must not be employed. SHA2 family (384 bits and 512 bits) should be used instead.

- 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.

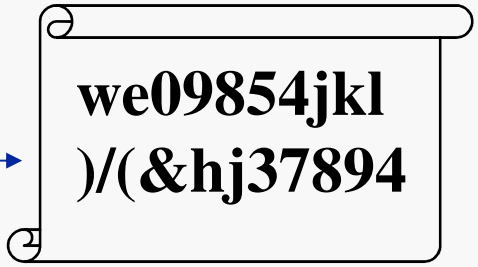
Digital signature

Hash value

plaintext



Apply hash function
Secure Hash Algorithm (SHA)

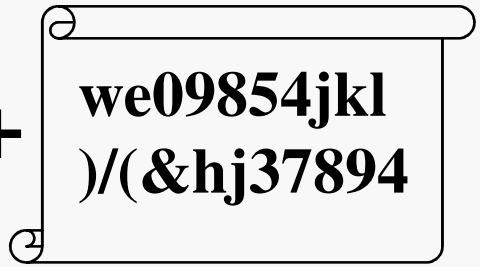


160 bits

Alice encrypts the hash value with her private (secret) key

Hash value

+



=

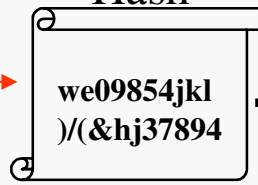
of Alice

Scenario #2 The integrity: Digital Signature

ALICE

1)

plaintext



Alice

+

Alice encrypts
the hash value with
her private (secret) key.

=

of Alice

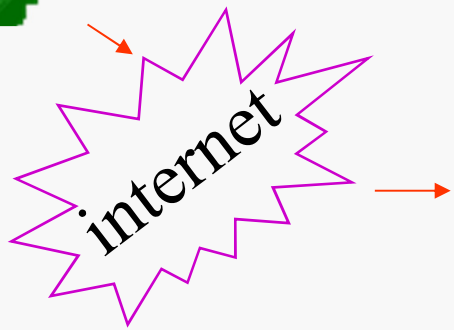
2)

plaintext

+

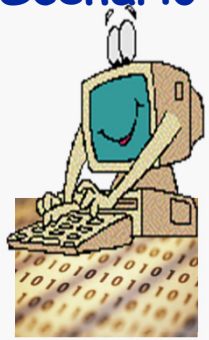
of Alice

Alice encrypts with
Bob's public key



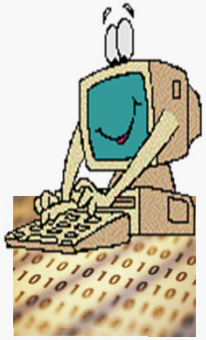
Scenario #2 The integrity: Digital Signature

BOB

1) 

Bob decrypts with his private(secret) key

= DIGITAL SIGNATURE of Alice + Buy the items and send them... plaintext

2) 

Bob decrypts with Alice's public key

+ DIGITAL SIGNATURE of Alice = Hash we09854jkl)/(&hj37894 Alice

3) 

Hash function + Buy the items and send them... plaintext = Hash we09854jkl)/(&hj37894 Bob

4) Hash we09854jkl)/(&hj37894 Bob ? = Hash we09854jkl)/(&hj37894 Alice

YES: done!

NO: cancel the transaction

The chain is only as strong as its weakest link...

Man-in-the-Middle Attack

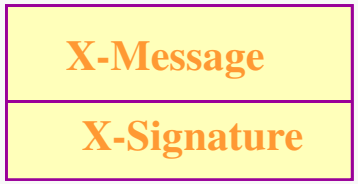
A

Original A
Message is signed with
A's secret key.

X : Attack

Bogus X
Message is signed with
X's secret key.

B



B reads the message with
X's Public key.
B assumes that the message is coming from A, while actually reading the message of X.

Necessity: To bind the A's public key with the A's ID in such a way that B completely trusts, meaning a Certificate !!!

The certification authority (CA)

Naming:

- Trust Center
- Trusted Third Party
- Certification Authority
- Nitelikli sertifika sağlayıcı

The function:

- Being used with the Public Key Cryptosystems.
- Provides the users with the security certification.

The definition for CA's

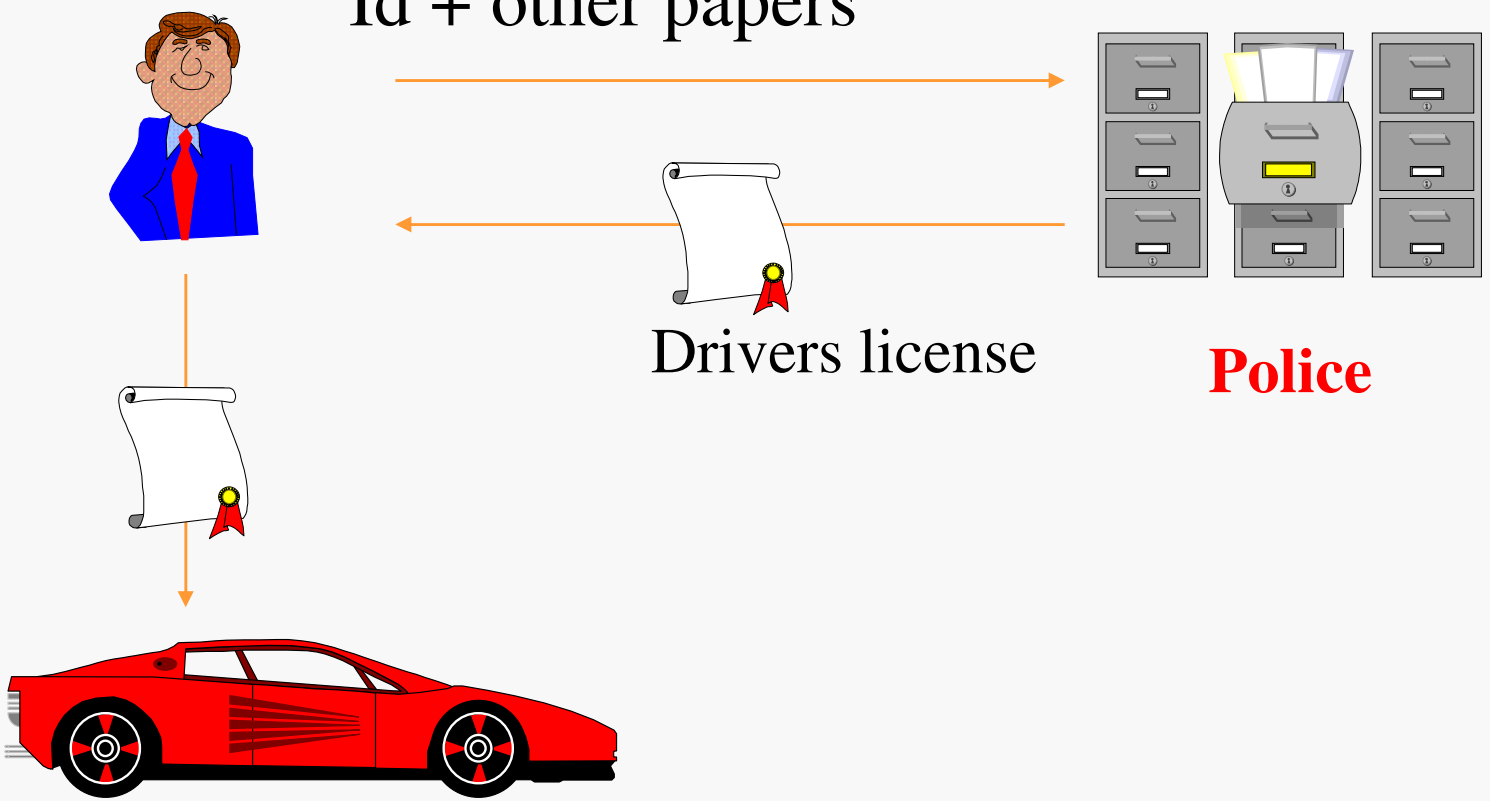
An agency which binds the public key of one person with the real identity of that person beyond any reasonable doubt.

The CA shall certify that bind with an appropriate certificate and be prepared to provide it to any real person and/or agency upon request, plus will be responsible for the actions of storing, revoking, cancelling and of updating the certificates securely and reliably.

Koltuksuz, 1998.

The certification authority (CA)

An analogy #1

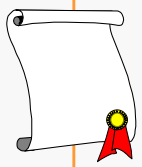


An analogy #2

Id + photo + other papers

Police

Passport

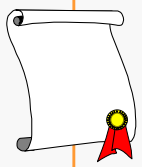


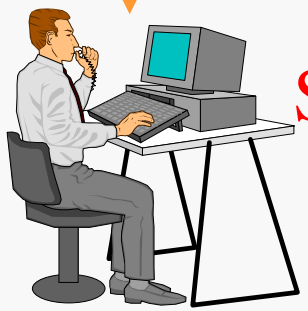
The certification authority (CA)

Id + **Public key**

certificate

Certification Authority





Secure e-commerce

The certification

Certificate binds the public key and the real person securely and reliably.

The digital signature of the CA shows that the certificate is authentic!

Name: Alice

Public key : hjgf89054her

Validity: 1/1/2007 - 1/1/2009

Certificate #: 4737

Issued by: CA's name

signature: CA's digital signature

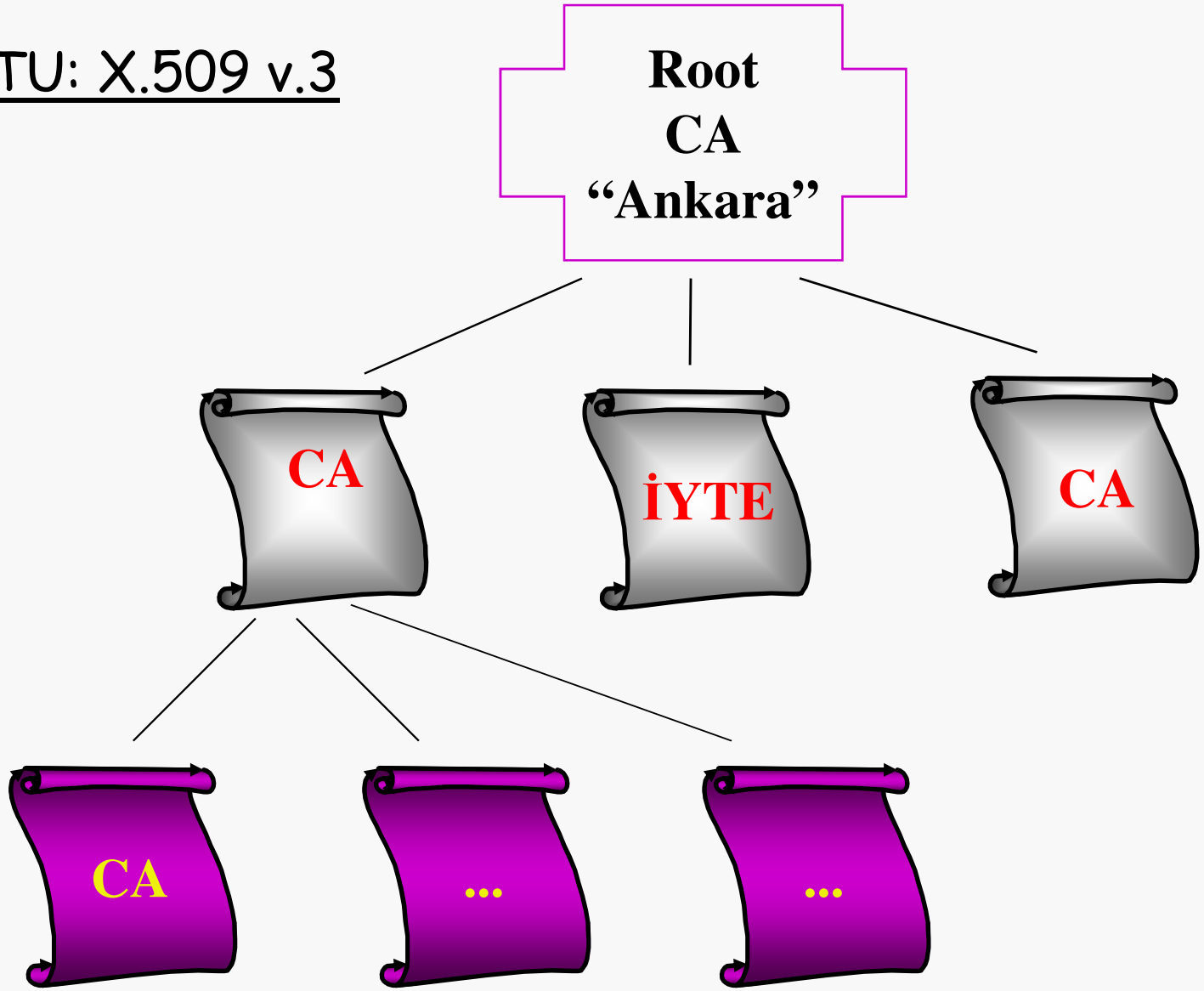
Certificates can be stored on disk, floppy, smart and/or optical cards and, on tokens and flash memories as well.

ITU

X.509 v.3 certificate

The certification

ITU: X.509 v.3



5070 sayılı Elektronik İmza Kanunu (EİK)

m.3 Elektronik imza

Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri.

m.4 Güvenli elektronik imza

a) Münhasıran imza sahibine bağlı olan,
b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,
c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,
d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan,
Elektronik imzadır.

Scenario #3 Authenticity

- Using asymmetrical encryption in a superimposed fashion for the purpose of ID control.
- Means that the sender encrypts with his/her secret key first, followed by the encryption with the receiver's public key.

Scenario #3 The authentication

ALICE

1) Buy the items and send them...
plaintext

→ Hash

we09854jkl
)/(&hj37894

Alice

+

Alice encrypts the hash value with her private (secret) key.

=

DIGITAL SIGNATURE

of Alice

2) Buy the items and send them...
plaintext

+

DIGITAL SIGNATURE

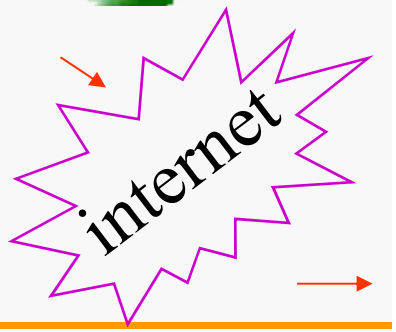
of Alice

→

Alice encrypts all with her private (secret) key.

→

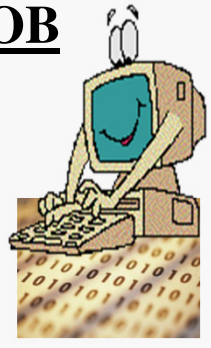
Alice encrypts With Bob's public key



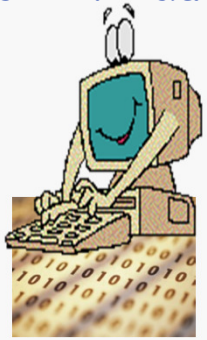
Scenario #3 The authentication

BOB

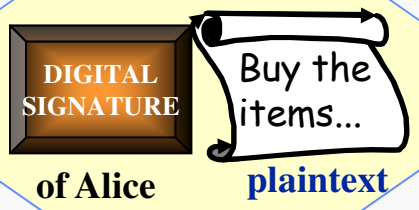
1)



Bob decrypts all with his **private(secret) key**



Bob decrypts all with Alice's **public key**



of Alice

plaintext

YES; continue.

NO

Cancel it! it's not AUTHENTIC!!!

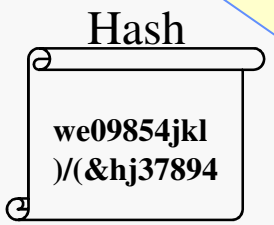
2)

Bob decrypts with Alice's **public key**

+

of Alice

=



Alice

3)

Hash function

+

plaintext

=

Bob

4)

Bob

?

=

Alice

YES: Done.

NO: Cancel the transaction!!!