WEB SECURITY – and Public Key Infrastructure

PALCO/RealSoft

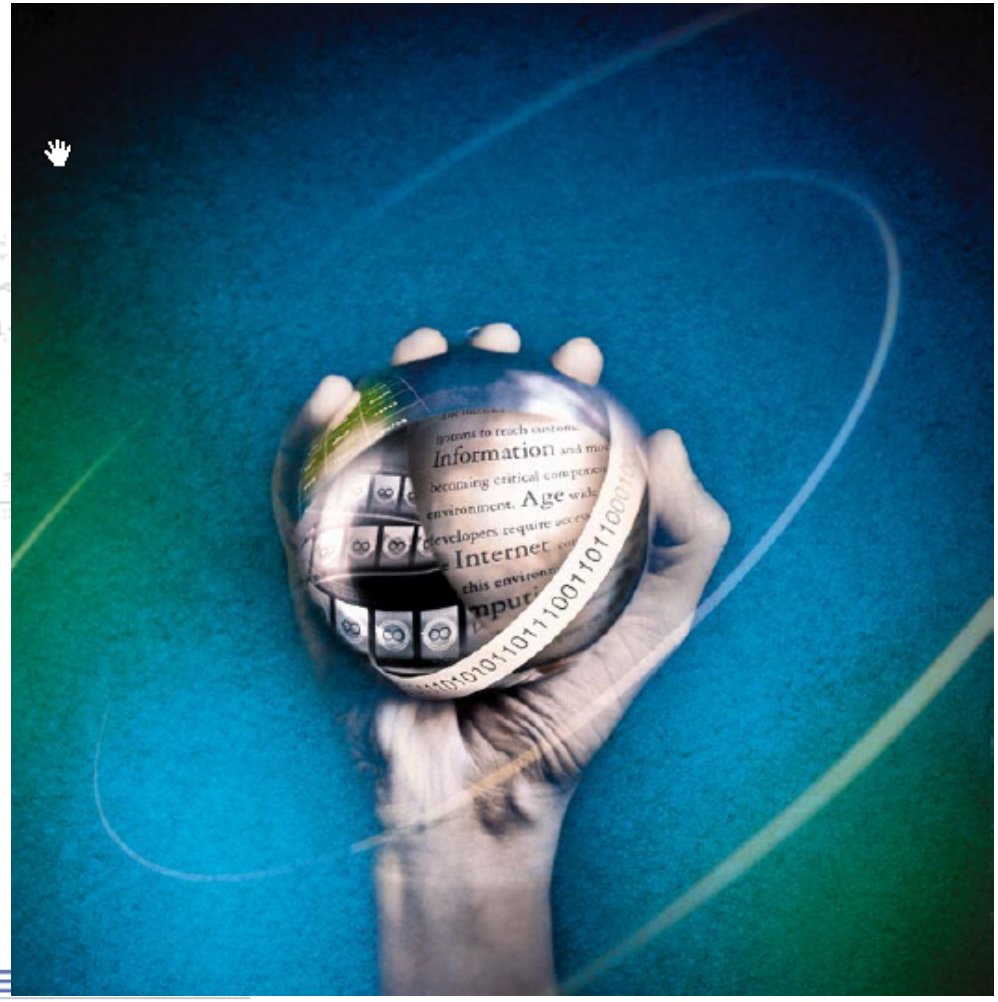
www.realsoft-me.com

www.palco.com.jo

Ammar Sajdi

Ammar.sajdi@realsoft-me.com

www.e-ammar.com



NOTE

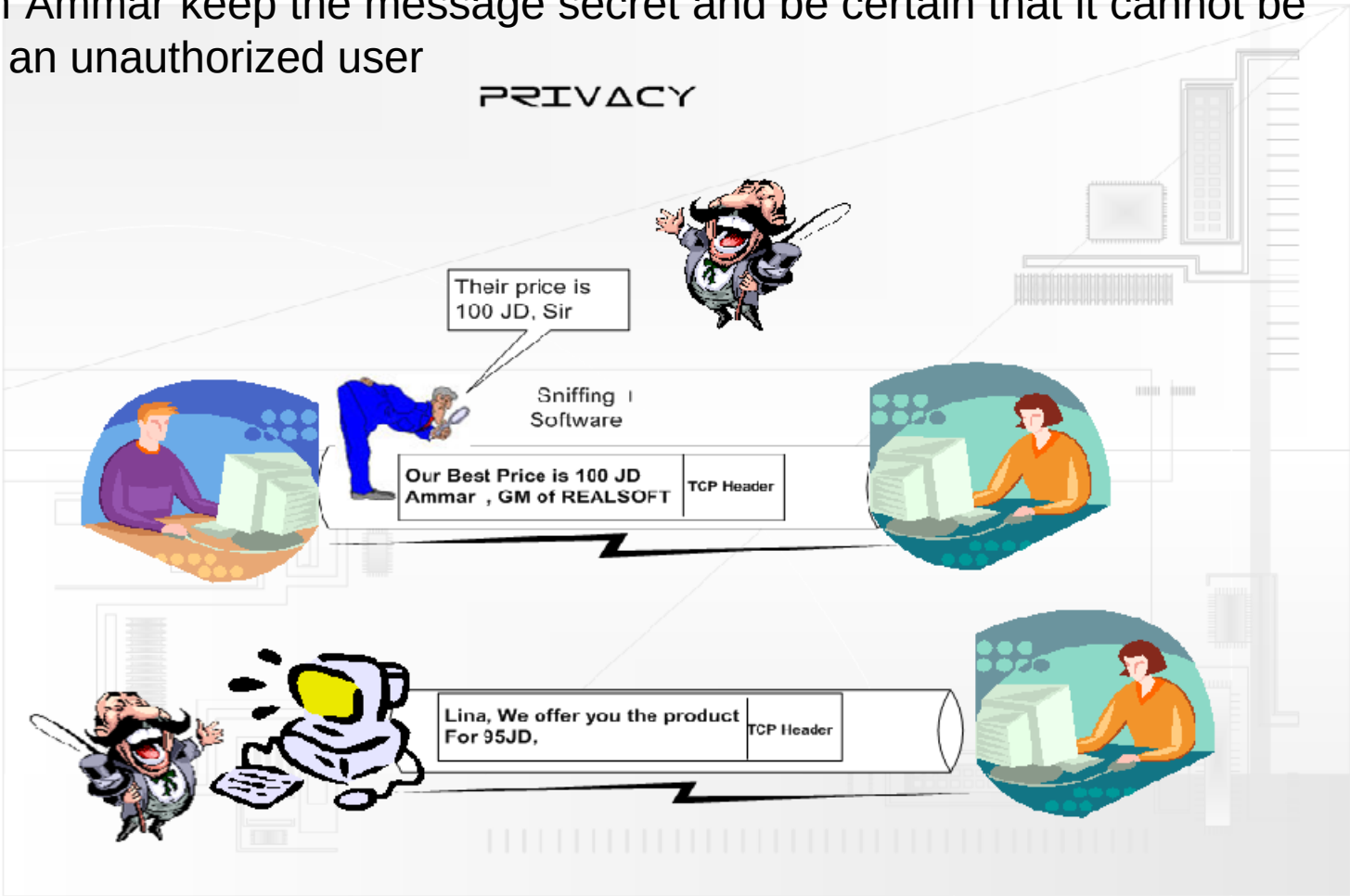
- **One of the GOALS of this lecture is to introduce Terminology (Jargon) used in WEB and Internet Security. (HACKER , CRACKER..)**
- **Many people use the terminology to impress others without understanding it, especially SALES people**

Top Myths of Security

- **Myth: Hackers cause most security breaches.**
- **Fact: 80% of data loss is to insiders.**
- **Myth: Encryption makes you secure.**
- **Fact: Security includes access control, data integrity, encryption, and auditing.**
- **Myth: Firewalls make you secure.**
- **Fact: 40% of Internet break-ins occur where there is a firewall in place.**

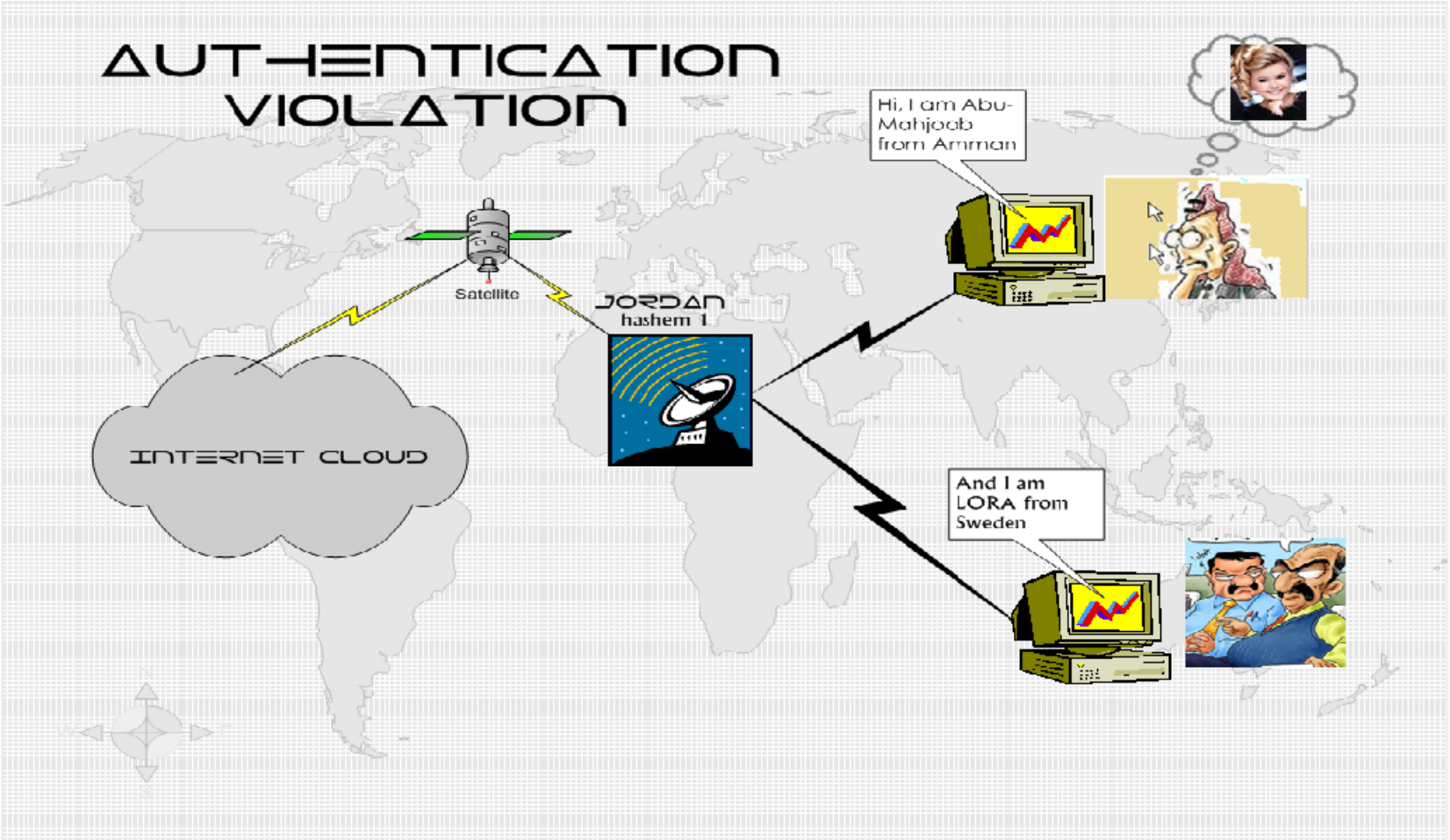
Privacy or Secrecy

How can Ammar keep the message secret and be certain that it cannot be seen by an unauthorized user



Authentication

How can Abu-Mahjoob be certain that the message originates from LORA

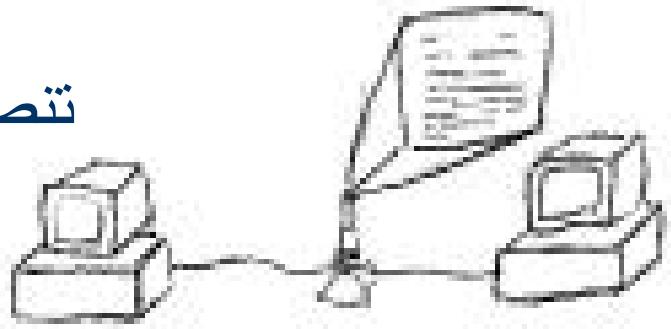


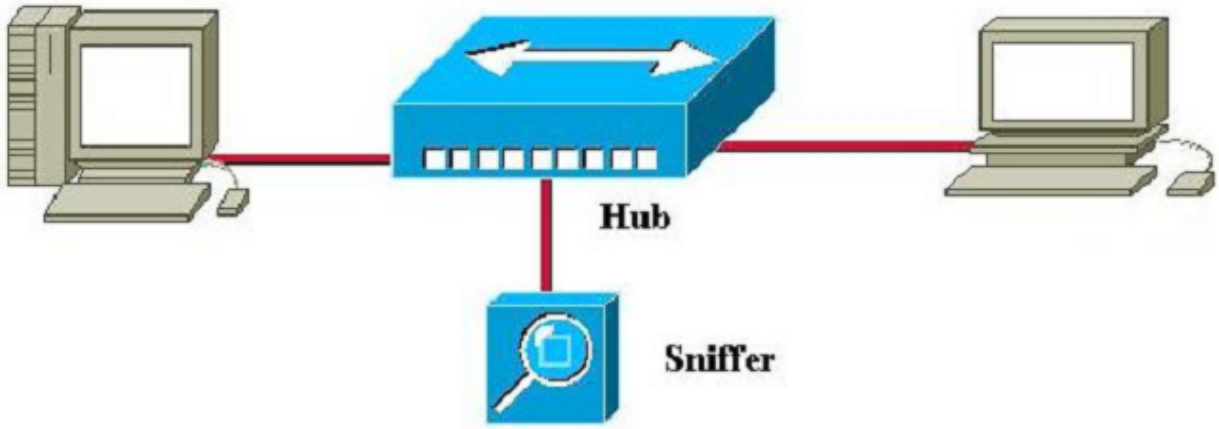
Sniffers - What it can mean

literally speaking

Also known as

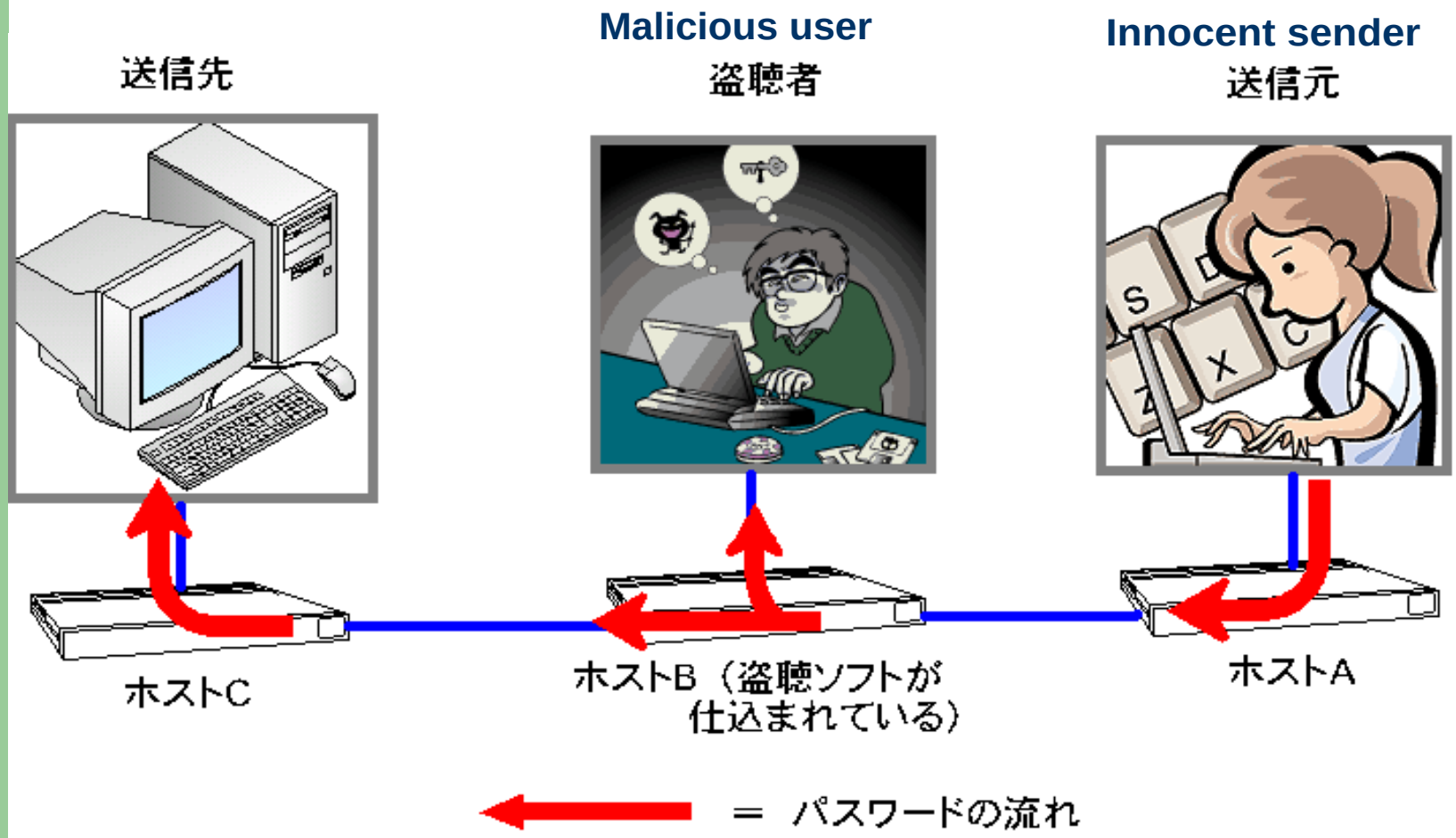
Eavesdropping تنصت





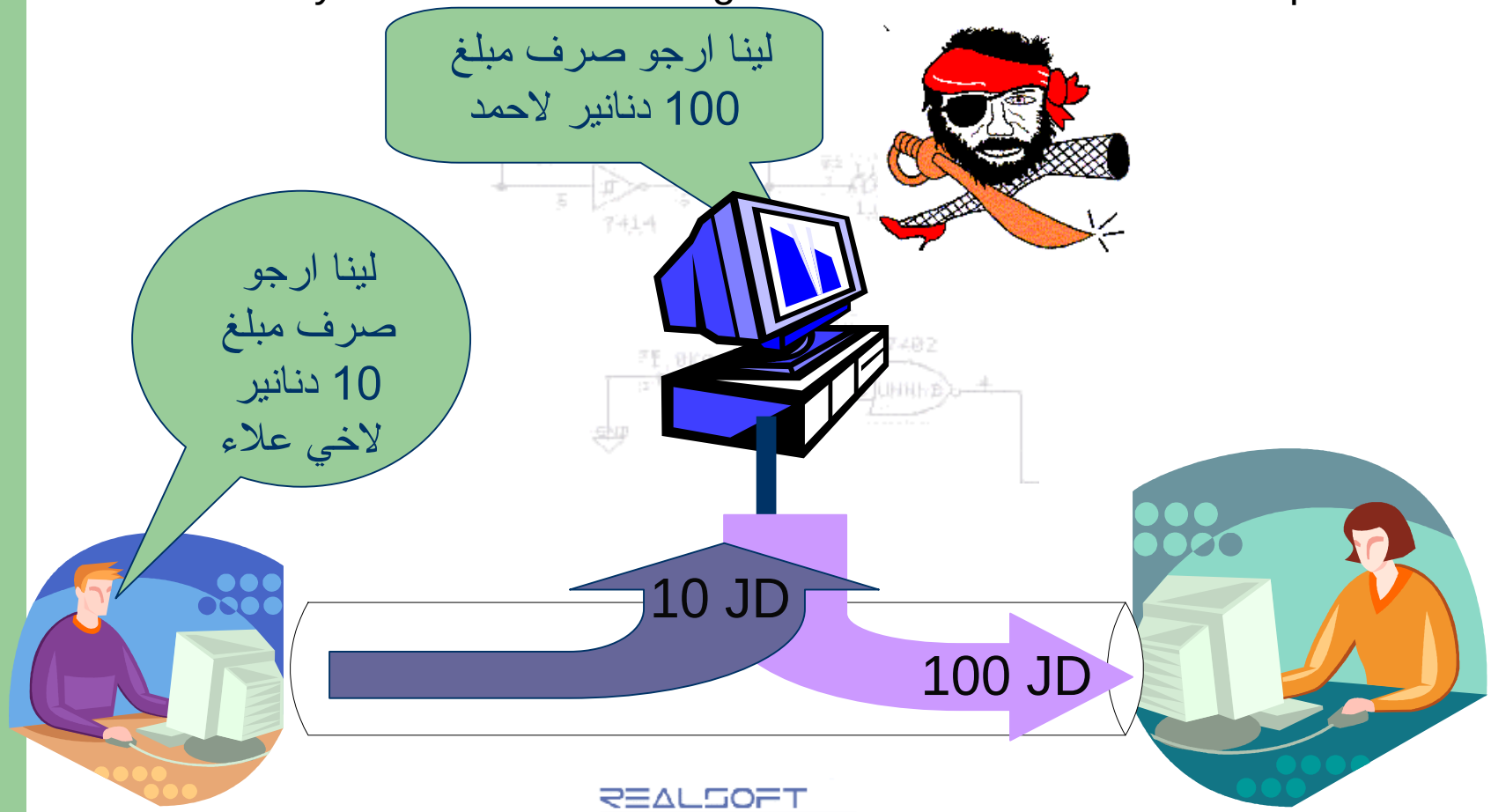
REALSOFT
ADVANCED APPLICATIONS

Japanese people also sniff



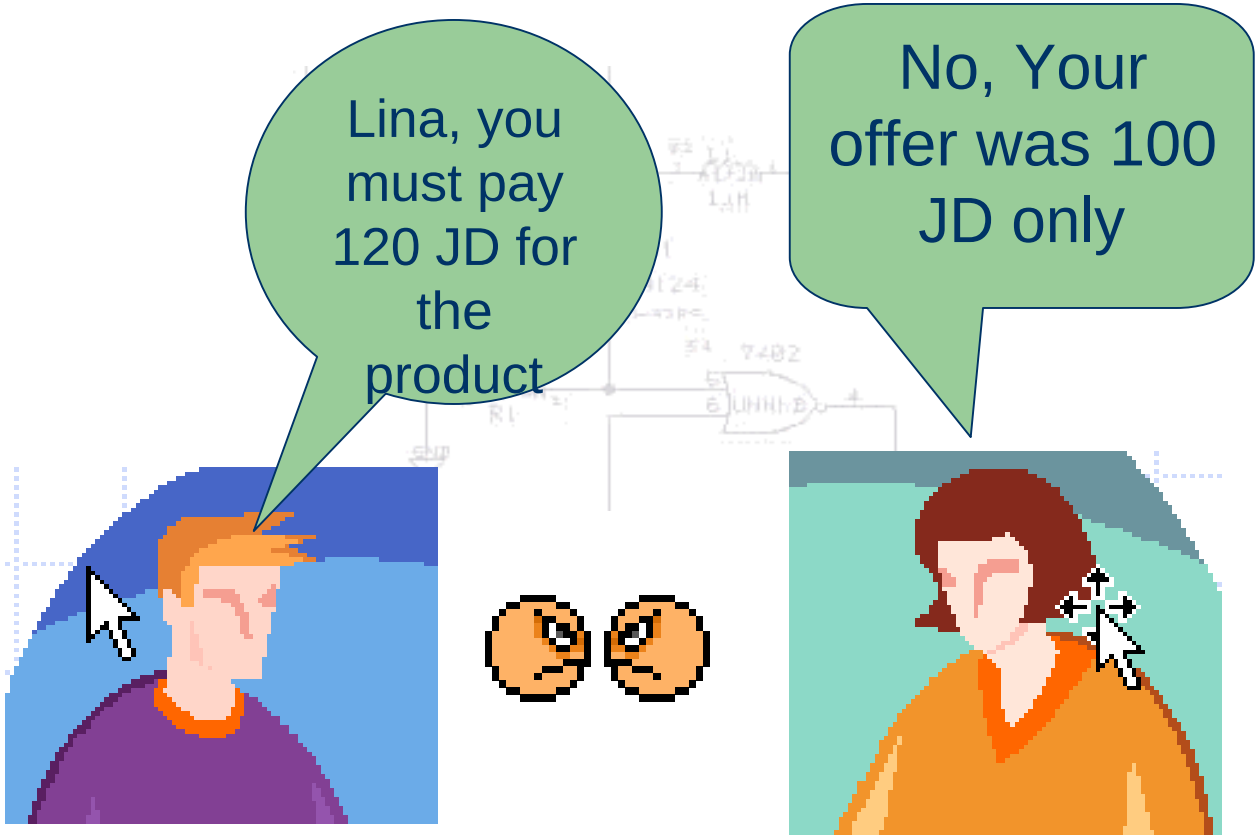
Integrity

How can Lina make sure that the message actually contains what Ammar Wanted to say. And the the message has not been altered or tampered with?



Non-repudiation:

How can Lina prove that Ammar must only ask for 100JD Agreed, I.e stopping Ammar from repudiating the agreement



Fundamental Security Requirements

- Authentication – التاكد من شخصية الاطراف الراغبة بالتواصل
- Privacy – حماية وسرية المعلومات من الكشف
- Integrity - ضمان عدم تعديل البيانات
- Non-Repudiation عدم قدرة التبرئ من المحتويات

All of the above concerns can be addressed by **PKI**, And that is why the next slides will discuss PKI in detail

Every day security in our society and workplaces

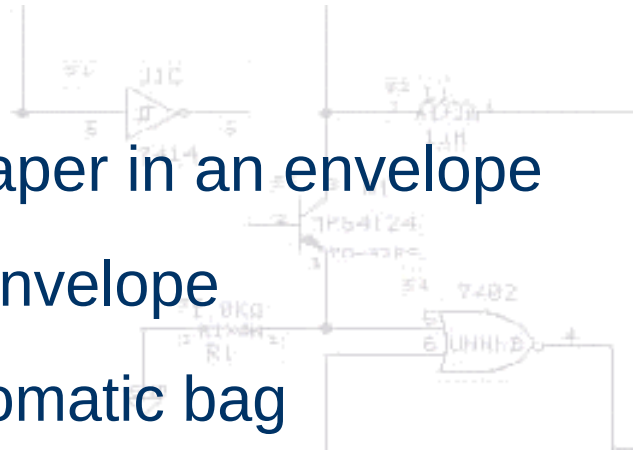
Societies have established an intricate set of laws and customs surrounding the use of Security services

To Identify someone, we ask him

- To Appear in Person, perhaps with some credentials (Passport, ID card etc ..)
- To be introduced by common and trustworthy acquaintance.

Privacy in society

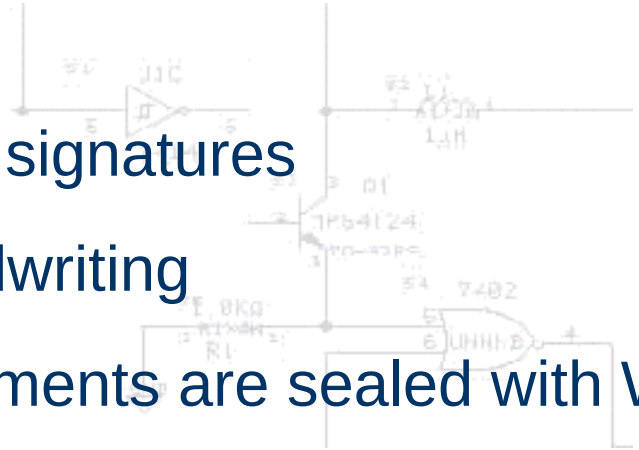
If we need to send a paper document securely (Privacy)



- Wrap the paper in an envelope
- Or double envelope
- Sealed diplomatic bag
- A strongbox with locks, keys, combinations and guard

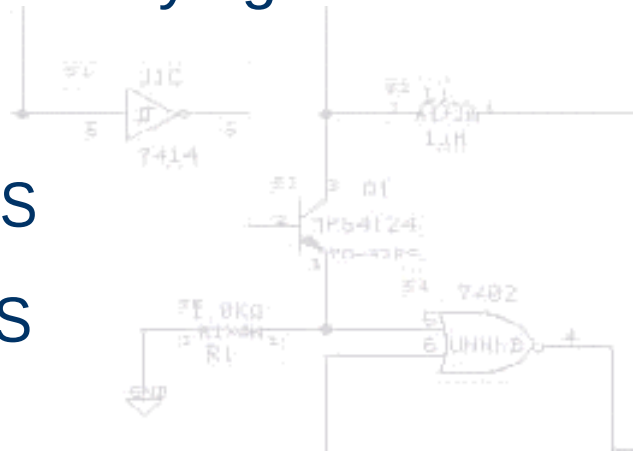
Integrity in society

- To verify the integrity of paper documents
  - Check their signatures
  - Check handwriting
  - Some documents are sealed with WAX, Stamped, or embossed.
  - Anti-forgery features are used in money/cheques



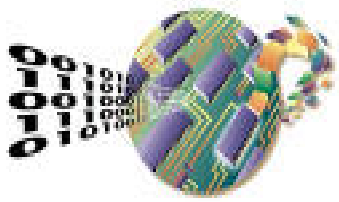
Non-Repudiation in society

To prevent either the sender or the receiver of a transaction from denying that it occurred



- CONTRACTS
- WITNESSES
- RECEIPT

In the Electronic World of Ours



In the digital world we live, many of the old, “Paper World” mechanisms are not possible

We may never get to meet the recipients of our electronic messages (face to face)

All electronic documents look the same – “zeros & ones” and therefore easily forgeable

We need services to replace Locks, keys, envelopes, signatures, credentials, etc

Why PKI

- PKI is seen as the most effective and cost effective technology for providing secure and authenticated transfer of digital communication
- PKI scales with a large number of users, organizations, sites, and applications
- PKI is being adopted as the security basis of most network-based commercial services e.g..
  - Electronic commerce, MasterCard, Visa, Netscape, Microsoft, Oracle, and many Online banking (BankAmerica, Arab Bank, etc ..)

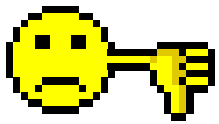
PKI Definitions

PKI stands for Public Key Infrastructure

INFRASTRUCTURE

ماذا؟ بنية تحتية؟

هل هذا يعني تصميم ومخططات؟



كوابل و حفريات؟

حكومة و عطاءات؟

ام صرف صحي ومجاري وعبارات؟

PKI is a SYSTEM that:

- ✓Verifies the identity and authority of Each Party involved in any Electronic Transaction (Internet, Intranet etc..)
- ✓Includes functions and technologies :-
  - •Public Key Encryption
  - •Digital Certificates
  - •Certification Authorities (CA)
  - •Registration Authorities.
  - •Certificate management
  - •Directory Services

PKI should still be unclear

•PKI is a set of components, people, policies and procedures which provides the foundation for the management of keys and certification used by Public Key-based security services.

•PKI assures the confidentiality of private key and the Integrity of the public key

It can include

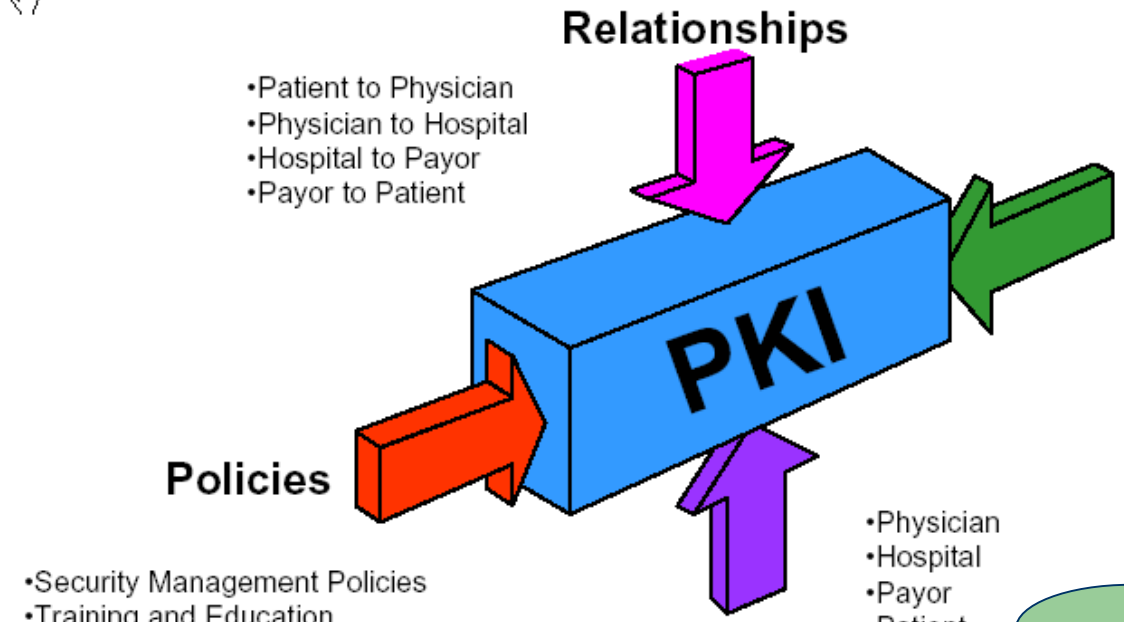
- Key generation and distribution
- Certificate Issuance and Distribution
- Certificate Validation

زاد الطين بلة، وما تؤلولي فهمتوا،
مفروض ما يكون مفهوم

www.Baltimore.com

Complete PKI

A Complete PKI



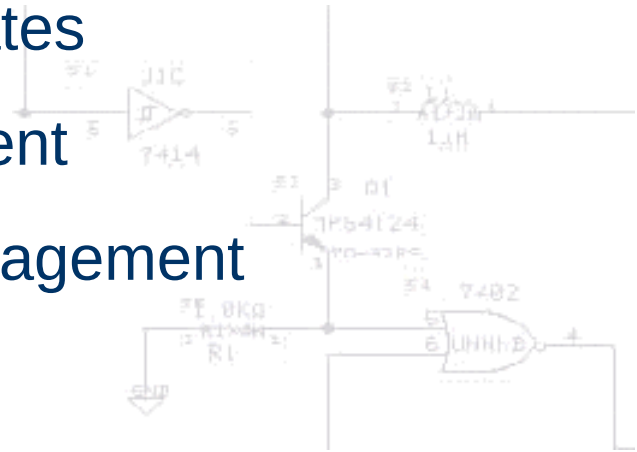
ما تخافوا راجعين ،بس ندرس اولTechnologies

A complete PKI is much more than technology

It is a careful blending of business processes, technology, policies and procedures

PKI Technologies

- Cryptography
- Digital Certificates
- Key management
- Certificate Management



Our discussion will focus on the first two

Cryptography

Two type of Key Cryptography

Secret Key (Symmetric Cryptography)

Public key (Asymmetric Cryptography)

Symmetric example

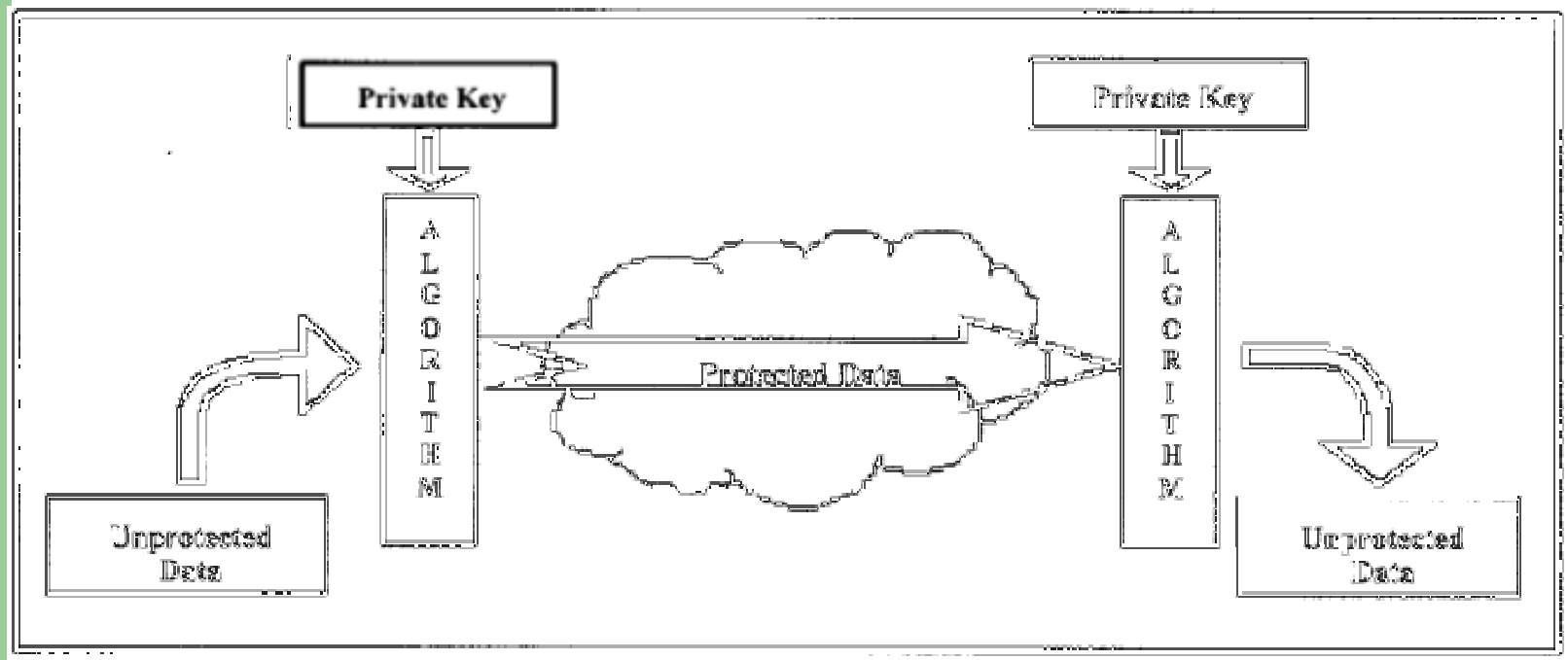


Fig. 2: Public key cryptographic system.

Conventional (Symmetric)

- One key only
- Used by both sender and receiver; the same key is used for encryption and decryption
- Must be protected by both sender and receiver, and kept private.
- Secure distribution of the key to the receiver is a challenge
- Receiver must not give the key to others!!!

Symmetric key Algorithms

Secret Key Block Ciphers

DES - Digital Encryption Standard - public & in common use - 64-bit block, 56-bit key.

Triple DES - Runs DES algorithm 3 times - more secure (E<k3>(D<k2> (E<k1>(data)))).

FEAL - from NTT, Japan - 64-bit key, variable strength.

RC2 - Recently published for public use by RSA; used for bulk encryption, variable length key (40-bit export).

IDEA - used in PGP - 128-bit key - patented.

CAST - Canadian public domain cipher (40-128-bit key)

Skipjack - NSA developed, secret algorithm, h/w only - 80-bit key incorporating key escrow.

GOST - Russian cipher - 256-bit key.

Blowfish - Bruce Schneier's algorithm, fast & compact, variable length key.

SAFER - Cylink cipher - 64/128-bit key

A Word about DES

•In 1972, the National Institute of Standards and Technology decided that a strong cryptographic algorithm was needed

•In 1974 IBM submitted the Lucifer algorithm

•NIST enlisted the help of the National Security Agency to evaluate the security of Lucifer

•there was initially a certain degree of skepticism regarding the analysis of Lucifer

•One of the greatest worries was that the key length, originally 128 bits, was reduced to just 56 bits, weakening it significantly

More about DES

One of the greatest worries was that the key length, originally 128 bits, was reduced to just 56 bits, weakening it significantly.

The NSA was also accused of changing the algorithm to plant a "back door"

But these fears proved unjustified and no such back door has ever been found.

NIST abandoned their official endorsement of DES in 1997 and began work on a replacement, to be called the Advanced Encryption Standard (AES

However, DES is still widely used by financial services and other industries

Cracking DES - Brute Force

•In 1998 the Electronic Frontier Foundation won the RSA DES Challenge II-2 contest by breaking DES in less than 3 days.

•More recently, in early 1999, Distributed. Net used the DES Cracker and a worldwide network of nearly 100,000 PCs to win the RSA DES Challenge III in a record breaking 22 hours and 15 minutes

•for a cost of one million dollars a dedicated hardware device can be built that can search all possible DES keys in about 3.5 hours

http://www.tropsoft.com/strongenc/des.htm

Read this book

Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design

Preface

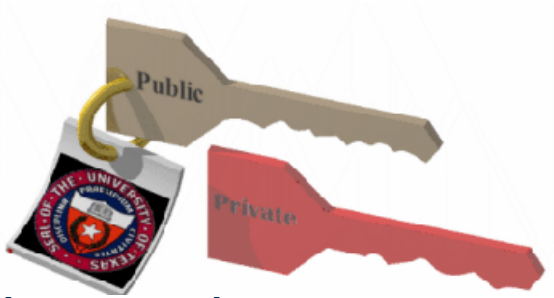
In privacy and computer security, real information is too hard to find. Most people don 't know what's really going on, and many people who do know aren't telling.

This book was written to reveal a hidden truth. The standard way that the US Government recommends that we make information secure and private, the "Data Encryption Standard" or DES, does not actually make that information secure or private. The government knows fairly simple ways to reveal the hidden information (called "cracking" or "breaking" DES).

…. There can be no more doubt. **DES is not secure.**

http://cryptome.org/cracking-des.htm

Public Key (Asymmetric)



- Two keys
- Mathematically related
- Each user has a unique key pair. One key used is used to encrypt and the other is used to decrypt
- One key is private (must be kept with you and remain secret, يعني confidential)
- The other is made public for others to know (The same way you make your phone number public for others to call you)

More about Cryptography

فكرت انو هذة المشكلة بس موجوده في symmetrical
، شكلي مش فاهم!

Symmetrical cryptography is orders of magnitude faster than Asymmetrical cryptography! WHY??

Public key technology (PKI) solves the key Exchange problem! Is there a problem anyway.

Cannot deduce private key from the public

Computationally complex

Asymmetric Cipher Algorithms

RSA – (Ronald Rivest, Adi Shamir, and Leonard Adleman)RSA's patented key exchange algorithm.

ElGamel – (Taher Elgamal) Digital Signatures and encryption.

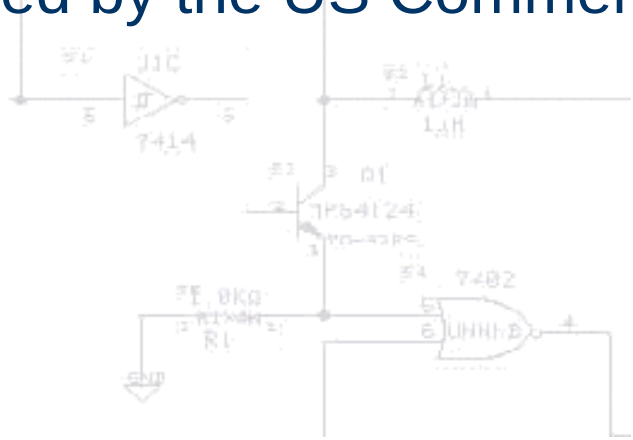
DSA - US Standard Digital Signature Algorithm - variant of ElGamel.

Elliptic Curve - Patent held by Certicom; based on finding an undefined point on a curve.

Diffie Hellman - The original key exchange algorithm - Stanford University -- patent just expired.

US Export Control Laws

•As of Late 1996, all programs that includes cryptography need to be licensed by the US Commerce Dept.



Back to excitement

How can Public key technology solve our information (data) related security concerns

Assumption:-

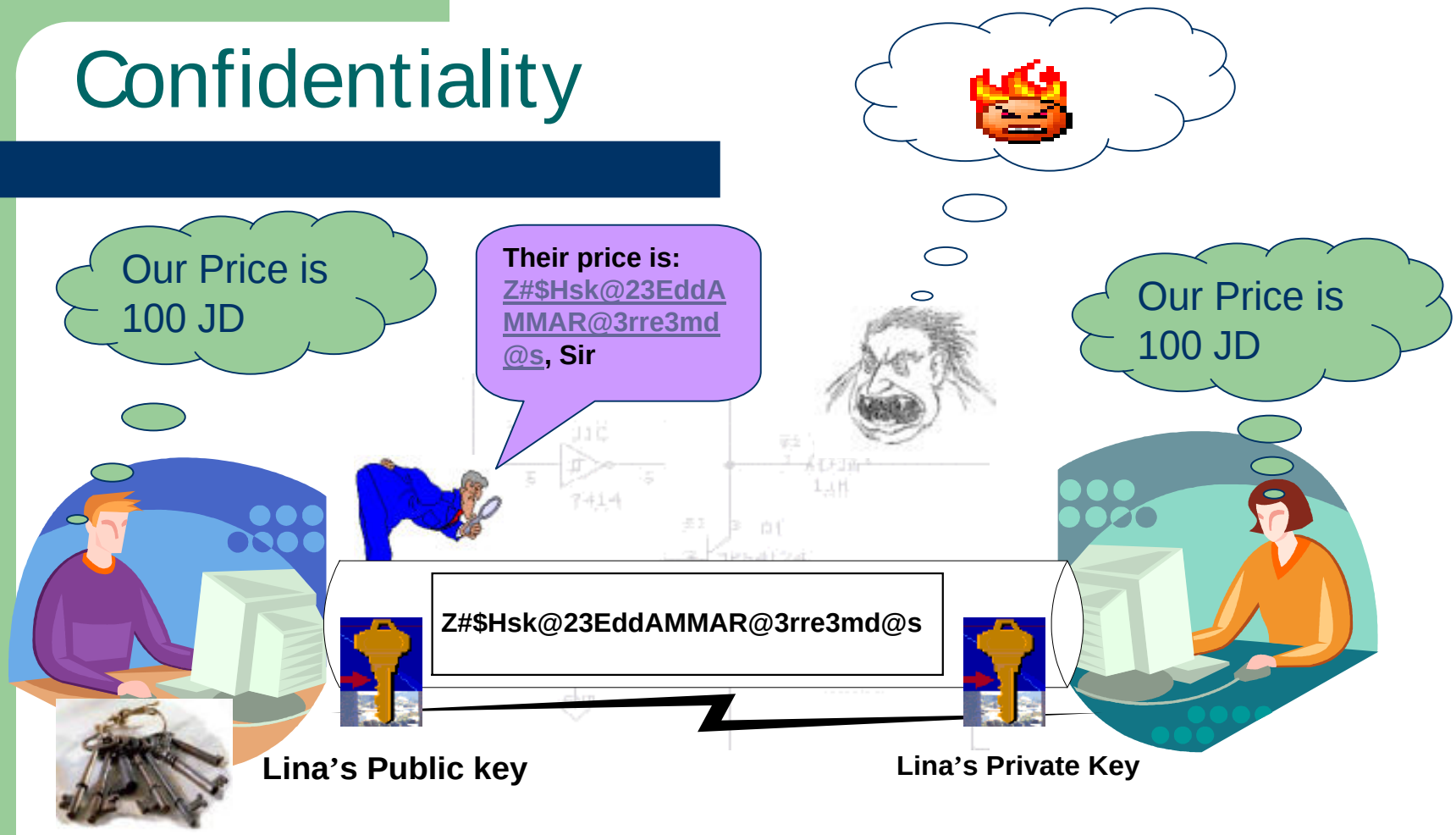
Ammar has generated his key pair

Lina has generated her key par

Ammar and Lina have exchanged their public keys.

Note: You may want to ask how the keys are exchanged???

Confidentiality



Would the same result be achieved if Ammar uses his private key to encrypt the message

Think of it this way

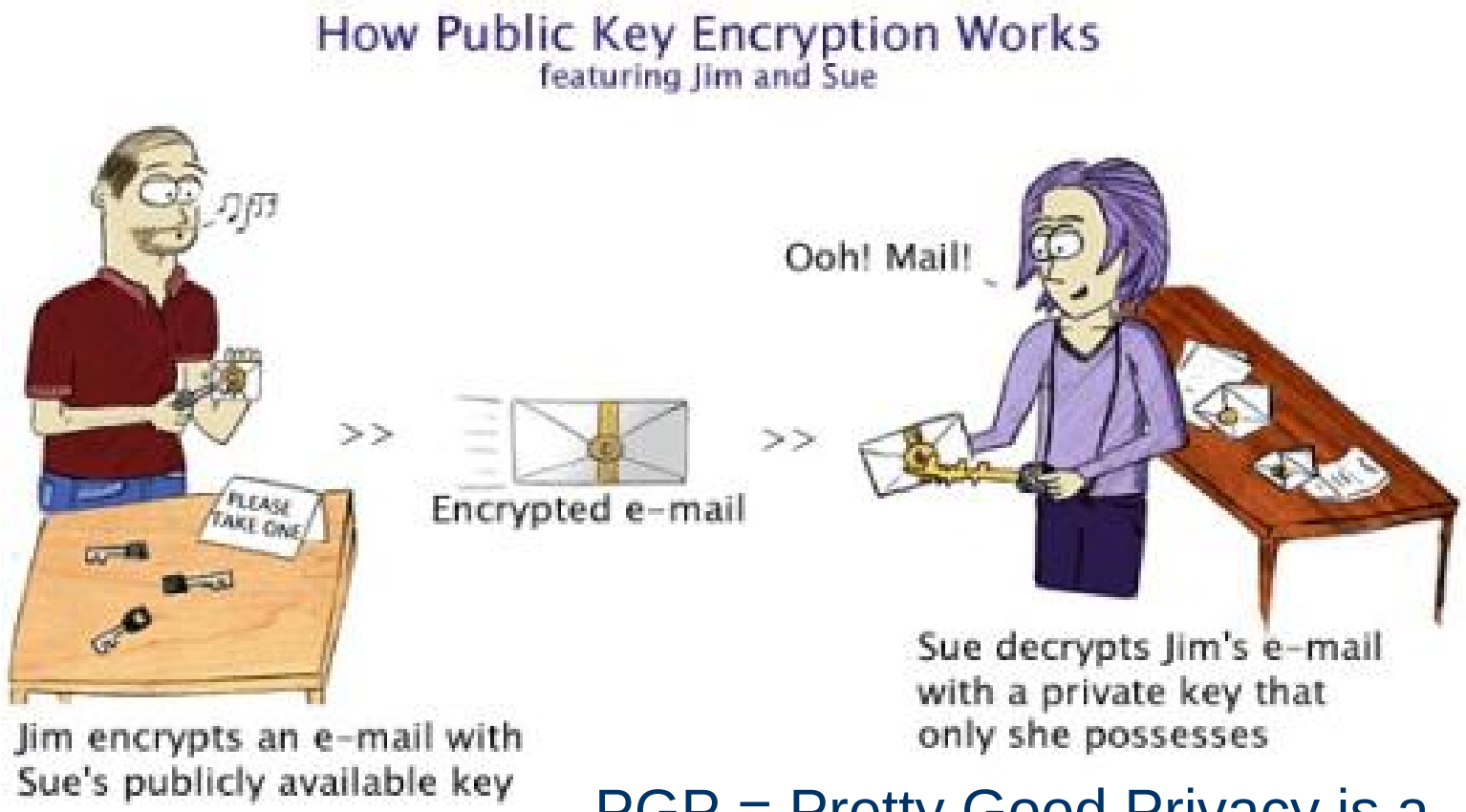
From All the selection of Keys، choose Lina's public key

Malicious cannot open the suitcase without Lina's Private key

Lina successfully opened the suitcase with her private key

لايمكن لاحد ان يفتح الشنطة الا لينا او من يملك مفتاحها الخاص

The Same applies to E-mail



PGP = Pretty Good Privacy is a popular Public key-based Software

REALSOFT
ADVANCED APPLICATIONS

Sender keeps many public keys

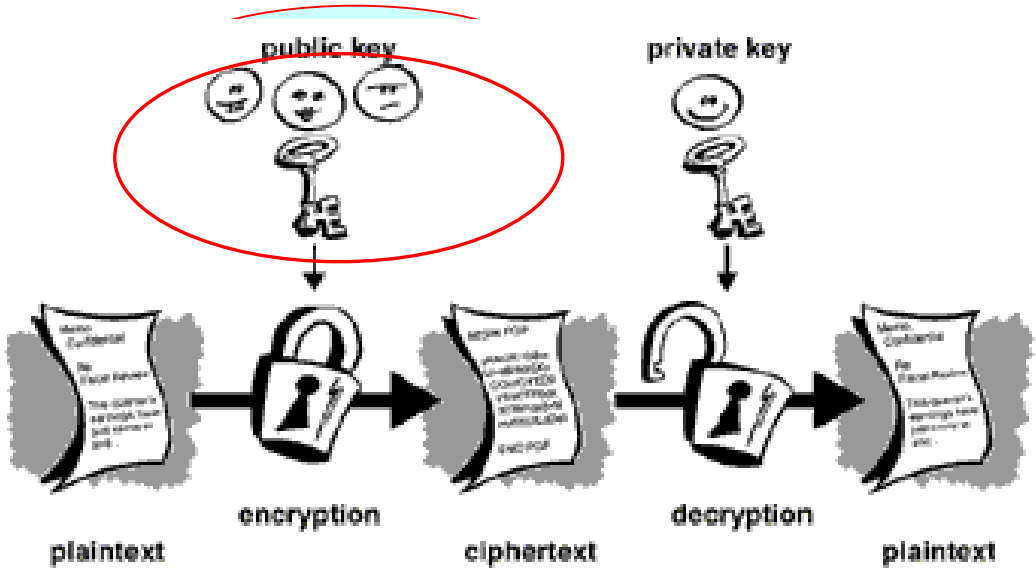
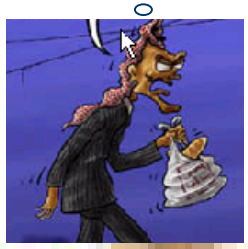


Figure 2-1. Public Key Cryptography diagram

Note that the sender may need to maintain many public keys each for a different user, Do you have any concerns about that!

Authentication

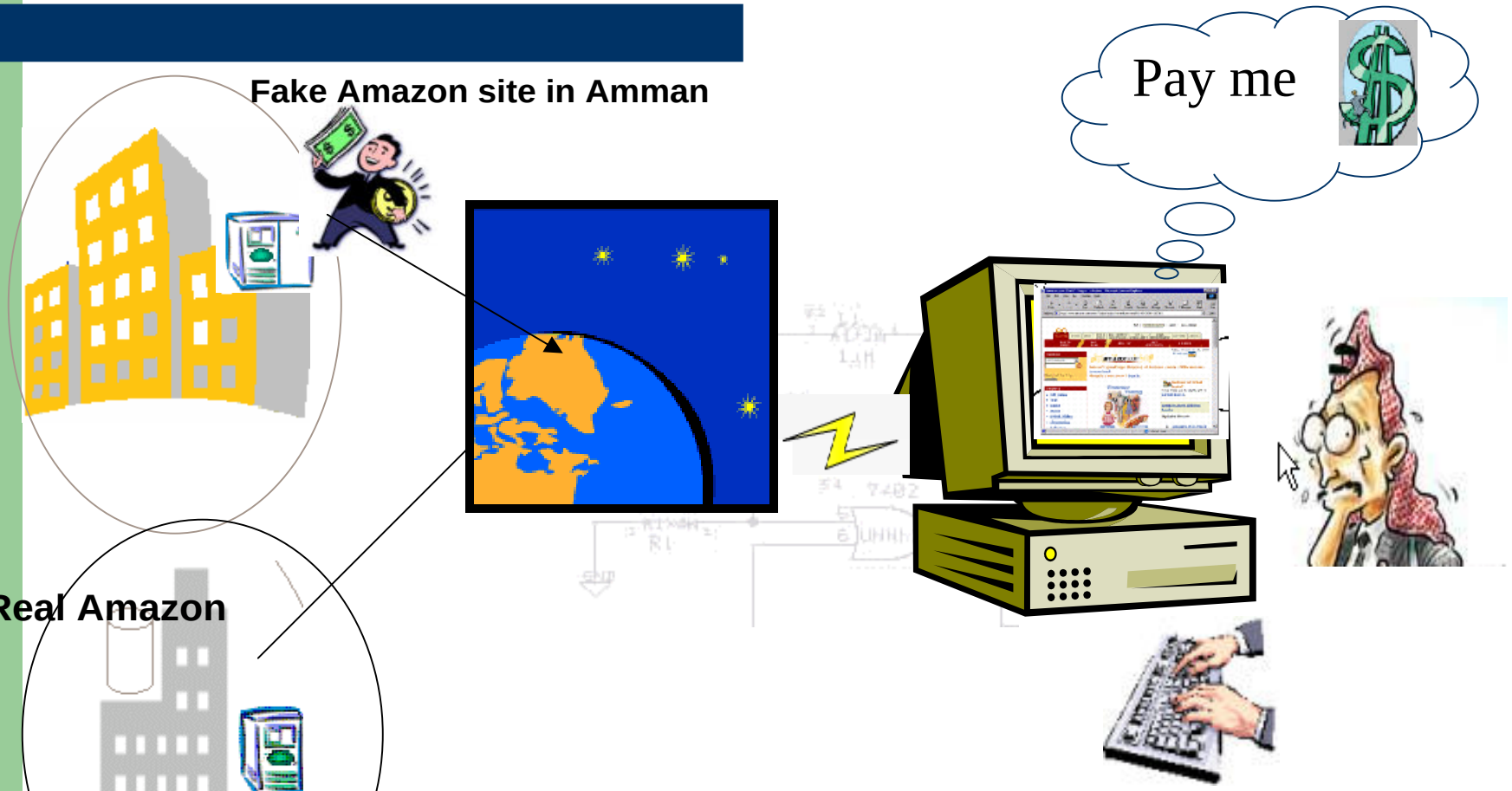
What can be the cost



OFT
ADVANCED APPLICATIONS

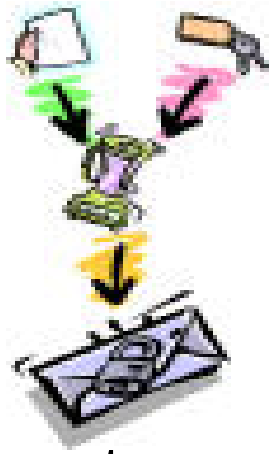
Authentication

What can be the cost



REALSOFT
ADVANCED APPLICATIONS

Solving Authentication Problem

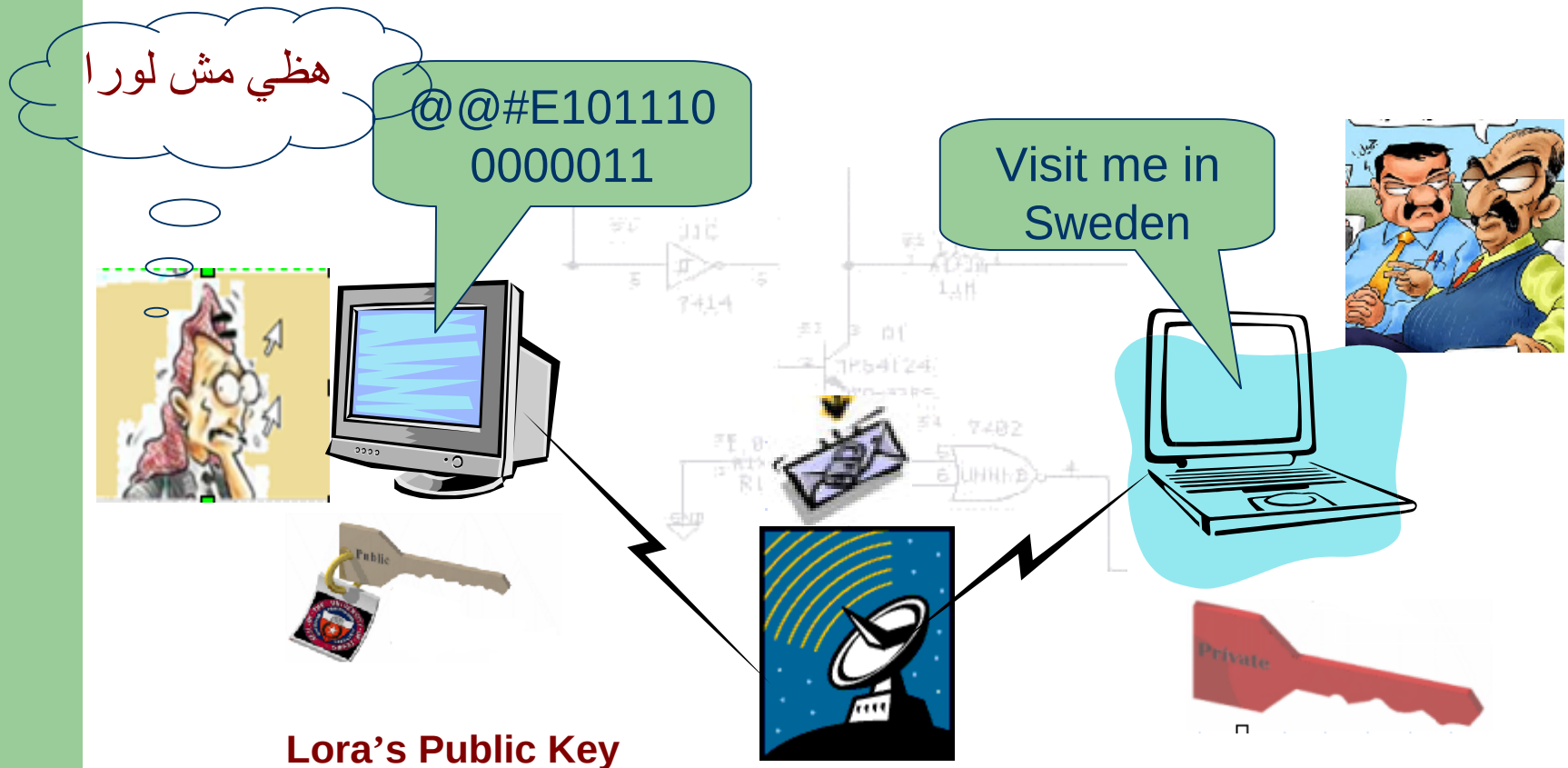


Ask Lora To send a message encrypted with her Private Key

Lora's Public Key is widely know, it is PUBLIC after all, Abu -Mahajoob has got a copy of it.

Note:- You may want to ask how he got the public key?

Sign me your letter please



Digital Signature – simple form

What he have seen in the previous slide is what is called digital signature

It is not a digitized image of the sender's hand written signature. It has nothing to do with real signatures

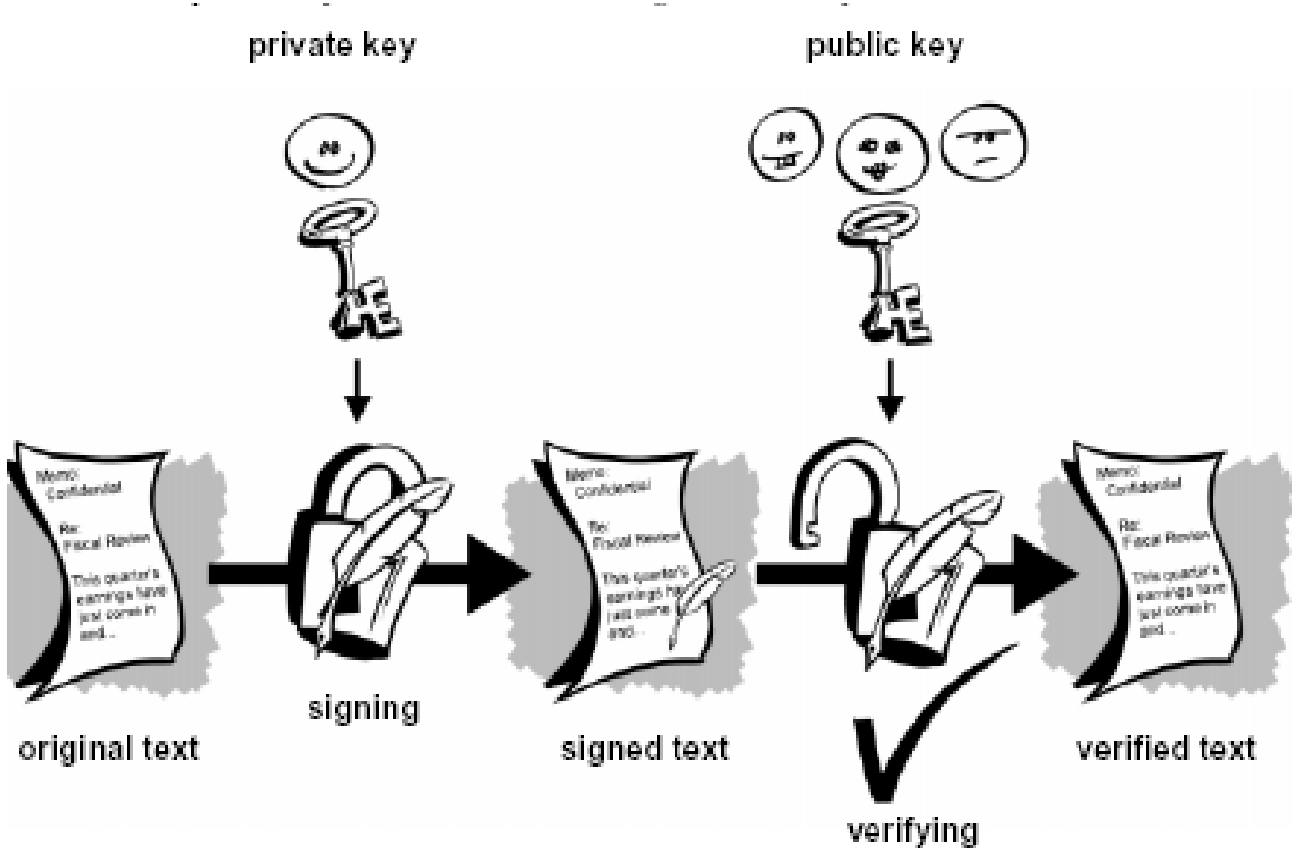
Sender uses private key to encrypt – the signing process

Receiver uses sender's public key to decrypt the signature

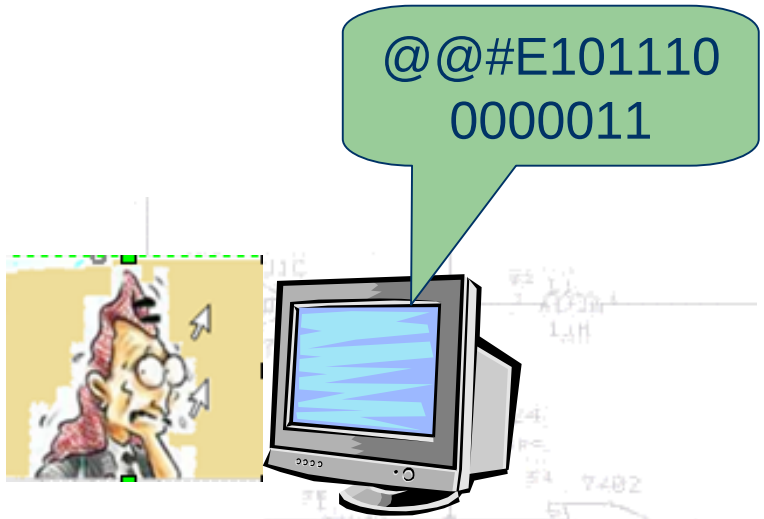
Binds the sender to the exact message contents, for non-repudiation

Does not provide confidentiality, Why?

Digital Signature – simple form

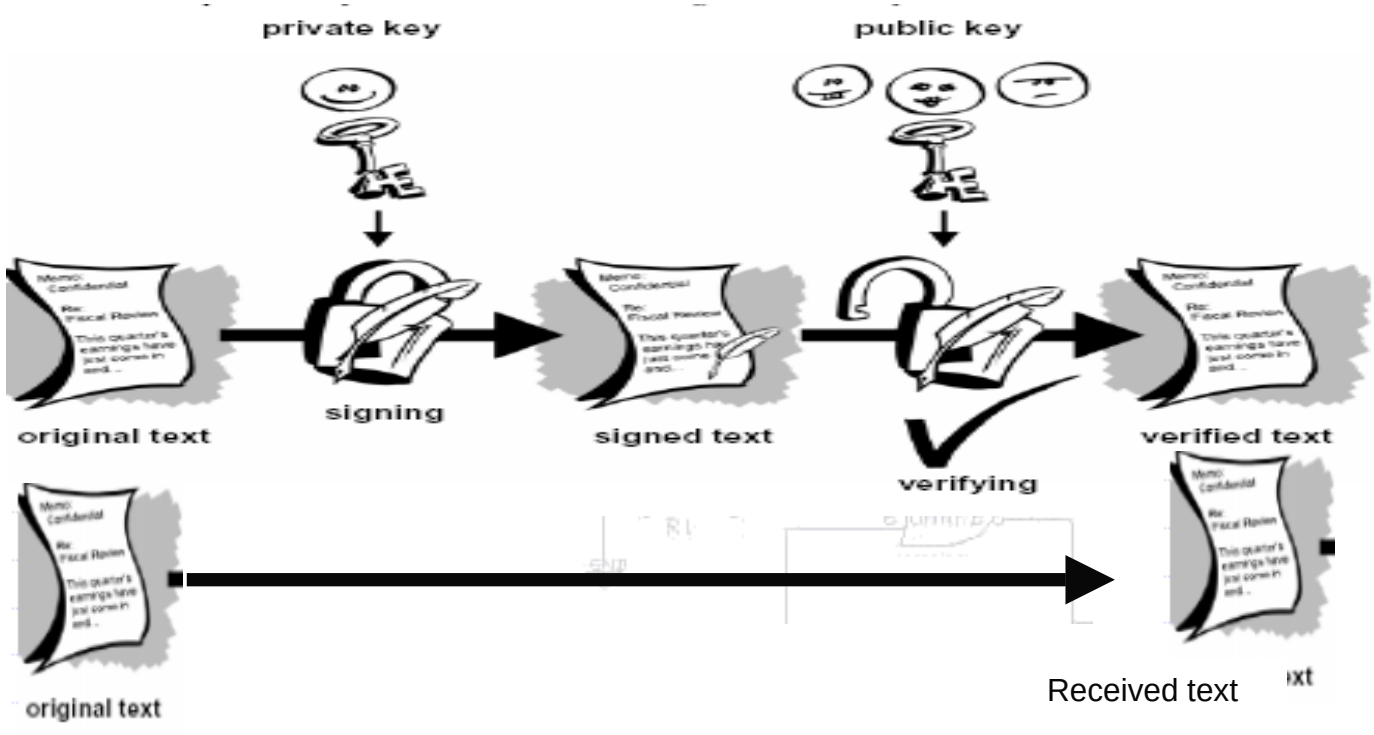


Simple Form is not enough?



Maybe “@@#E1011110000011” was really the sent message, just because he could not read it does not mean it is incorrect!!

Need to verify against the original text



The original Text is send non-encrypted. If the original text matches the verified text, it is a proof of the source and Integrity of Data

A better approach

The previous mechanisms dictates that the message is sent twice, once encrypted and another time un-encrypted (PLAIN) so that it can be compared with the signed copy.

Disadvantage is = Message size is now doubled

Solution : Use One way Hash Function as a verification mechanism

Message Digest

- Message Digest is the output ONE-WAY Hash Function

MD5 hash function example

MD5(ammar) → 4f3727280981617fef4287f449468977
MD5(bmmar) → 78a6d3f896b1a4c37ae9b8f39603dc8e
MD5(a) → 60b725f10c9c85c70d97880dfe8191b3

One way Hash Functions

Convert arbitrary length string to a fixed length output H=H(P)

Large input produces a small fixed length output

Trivial to produce H, given P

Extremely Difficult to obtain P from H – **One way**

Very Difficult to find two inputs , P1 and P2 that yield the same H (**Collision**)

A minor change in the input results in significant change in the hash

When computing a hash function for a message, the output is called the Message Digest – example is check sum

In other words

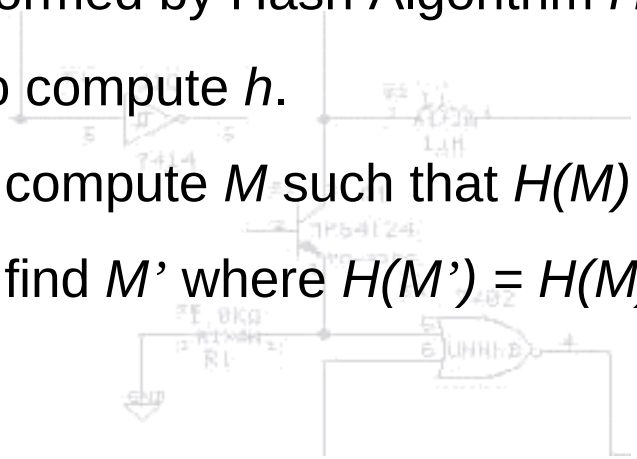
Message Digest or Hash

Message *M* is transformed by Hash Algorithm *H* to fixed length Hash *h*

Given *M*, it is easy to compute *h*.

Given *h*, it is hard to compute *M* such that *H(M) = h*

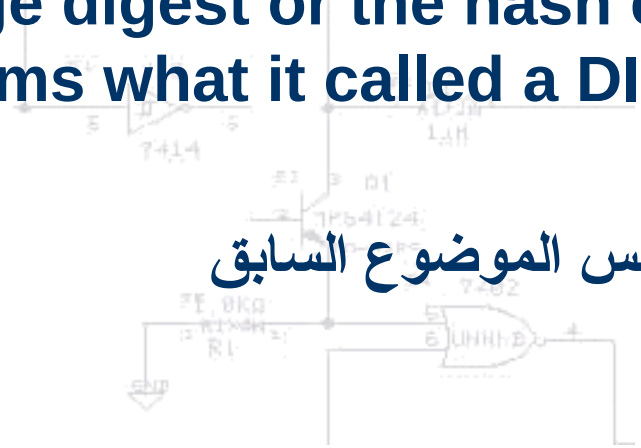
Given *M* it is hard to find *M'* where *H(M') = H(M)*



Digital Envelope

- **The message digest or the hash code of a message forms what it called a DIGITAL ENVELOPE**

فقط تسمية لنفس الموضوع السابق



Message Authentication Code, MAC

- **MAC is just the algorithm that results in the Hash Code or the Message Digest.**

Do not confuse this MAC with the MAC that is part of the Data Link Layer (OSI model)

Commonly known hash functions

•MD2, by Ronald Rivest, most secure, 128 bits, takes long to compute.

•MD4, Ronald Rivest. Fast alternative to MD2, 128 bits, shown to be insecure.

•MD5, Ronald Rivest, modification of MD4, 128 bits, in 1996 flaws were discovered that allowed collisions to be calculated, slowly flowing out of flavour.

•SHA, by NSA, the Secure Hash Algorithm, 160 Bits, NSA and NIST announced that the algorithm was not suitable.

•SHA-1, NSA, revised SHA.

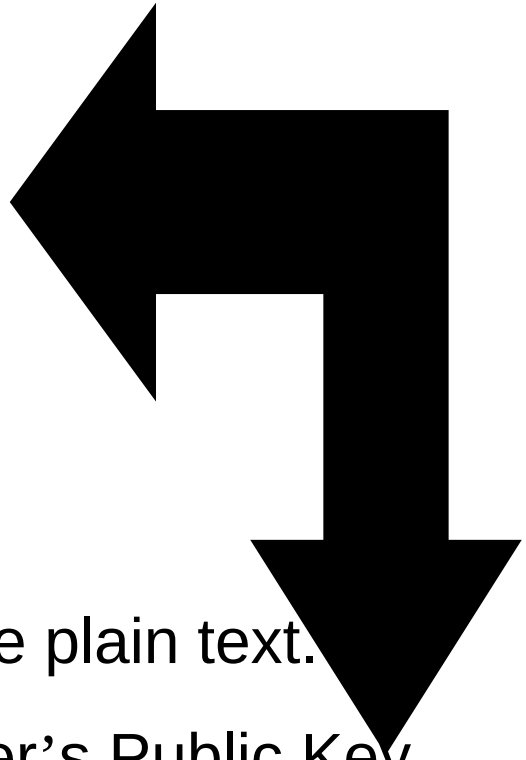
Advantages of Message Digest

- Much faster than traditional symmetric crypto.
- No patent restrictions. براءة اختراع
- No export restrictions.
- Used to create encryption keys by computing a user selected pass-phrase. PGP uses this technique.
- Used to create a digital signature.

The complete picture digital Signature

Sender

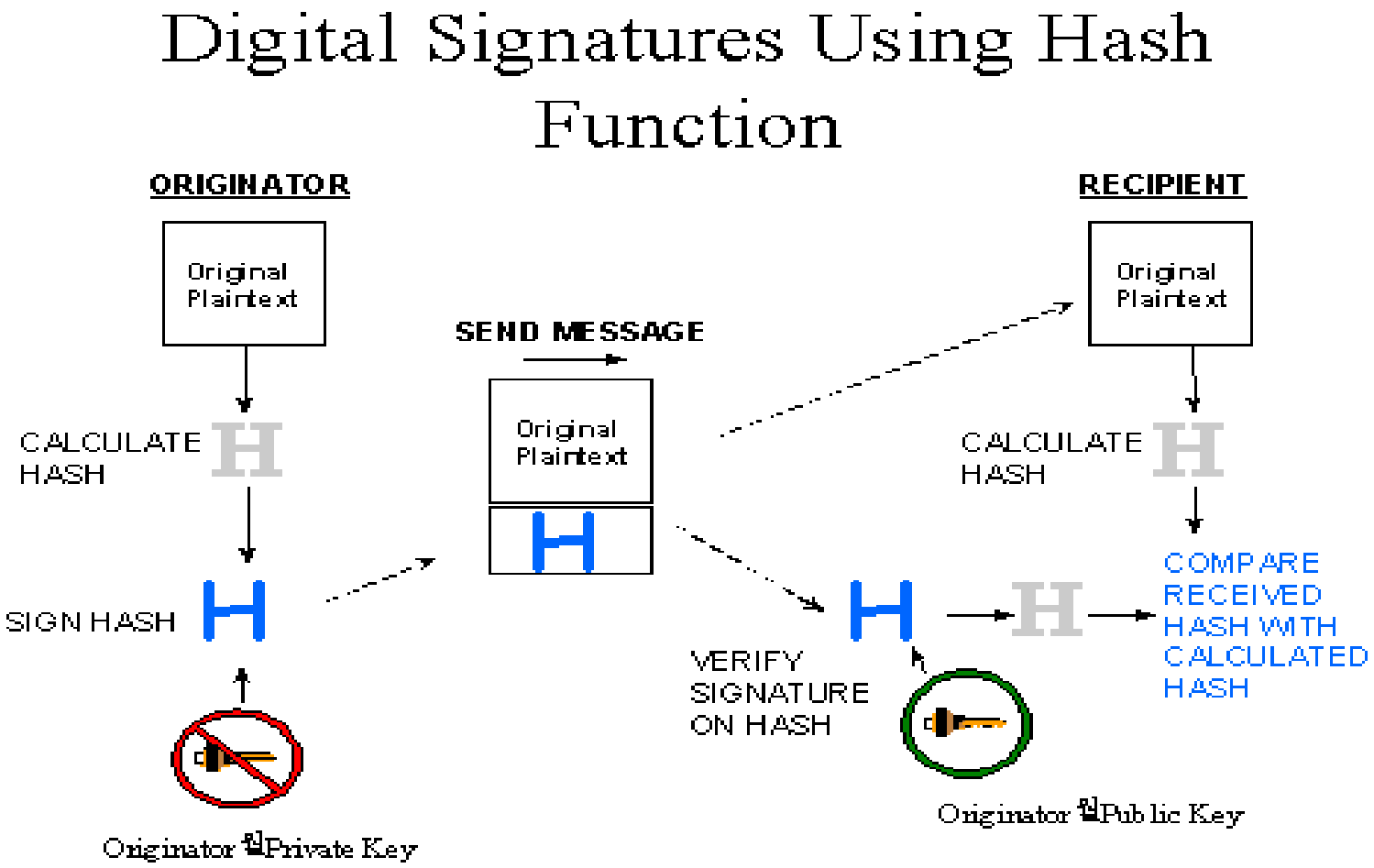
- Calculates “Message Digest”
- Encrypts digest with own Secret Key
- Appends it to message.
- Actual message not encrypted



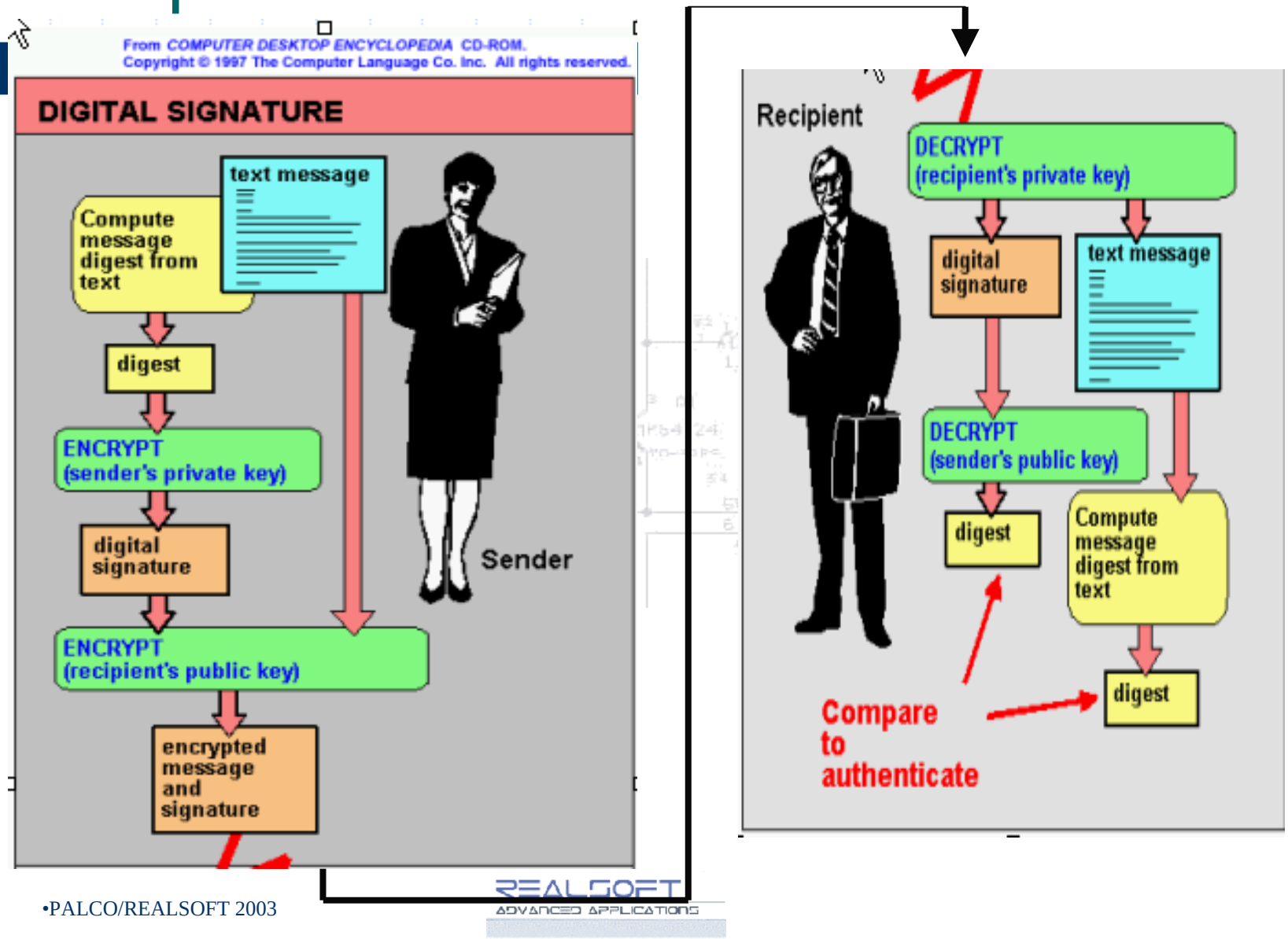
Receiver

- Calculates “Message Digest” from the plain text.
- Decrypts encrypted digest with Sender’s Public Key.
- Compares with calculated value

A picture of the complete picture -- Digital Signature



Explain This Please?



Concerns

Is the public Key I have is truly LORA's? Somebody might have given me the public key of another person and told me that it is LORA's

Authentication problem is, therefore, Not YET completely Solved. It is only solved if I am sure that the key I have is for LORA

This will lead us to introduce Digital Certificates.

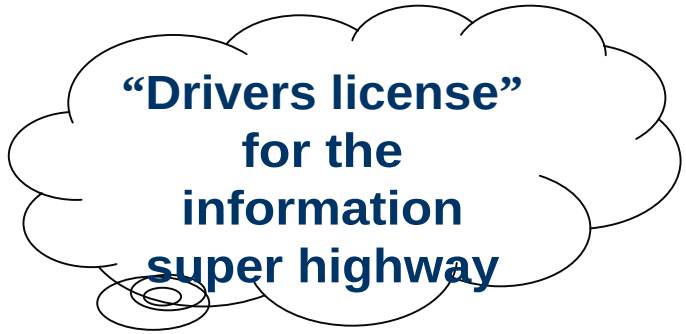
Need for Digital Certificates..

Verifying a digital signature requires

- Access to the signer's public key.
- Assurance that it really corresponds to the signer's private key

Some convincing strategy is necessary to reliably associate a particular person or entity to the key pair.

Digital Certificates



The idea: Passport Identification

You are identified by information (and a photo) issued by a highly trusted agency (وزارة الداخلية).

In the digital world, a digital certificate is an electronic document containing all personal details of a user (or Entity) and carries his public key.

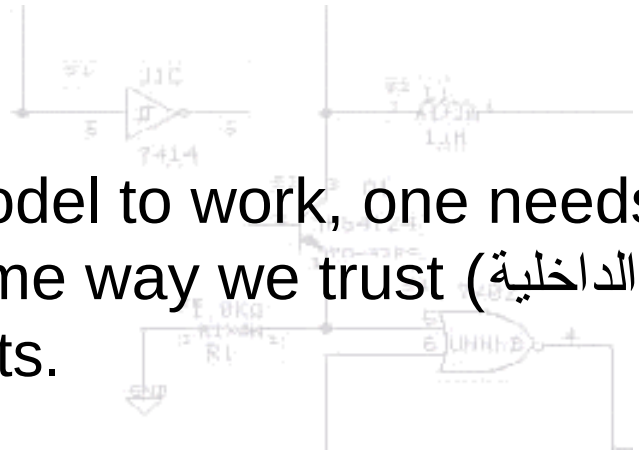
Issue by a Certification Authority (CA) after a proper verification of the applicant’s credentials by an affiliated Registration Authority (RA)

As defined by Computer Dict.

A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.

It is all about Trust?

The Certification Authority (CA) is trusted to verify and associate a key pair with a prospective signer (user)



For the PKI model to work, one needs to trust the CA exactly the same way we trust (وزارة الداخلية) when it issues passports.

To my knowledge, No CA in JORDAN.

What institution can you suggest to be a CA, Who do you TRUST?

Integrity of a Certificate

If you Trust a CA, they you trust the public key of the user for whom it is issued.

What about somebody maliciously compromising the integrity of the certificate itself?!! (changing its contents).

And how do you guarantee that this electronic documents was truly issued by the CA you trust and not by an impostor.(محتال)

You Know the Answer, tell me

REALSOFT
ADVANCED APPLICATIONS

Digital Certificates in Brief

Mainly to establish identity as follows

- You present a “Proof “ of identity.
- The CA verifies your identity with RA.
- The CA generates a public-private key pair.
- The private key is issued to you.
- Your public key is placed in a digital document that is then signed by the CA, and published (like phone book) in a public place (eg X.500 name server, **LDAP** or a WEB server)

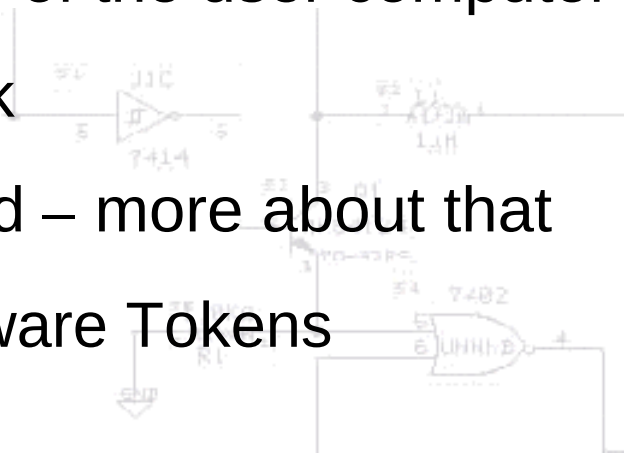
Where else to keep Certificates

On the Browser of the user computer

On a floppy disk

On a smart Card – more about that

On Other Hardware Tokens



Certificate Format X.509 V3

Version

Certificate serial number

Signature algorithm id

Issuer (CA) X.500 Name

Validity Period

Subject Name (User) x.500 Name

Public Key

Issuer Unique ID

Subject Unique ID

CA Signature

Example of a certificate

Certificate

REALSOFT
ADVANCED APPLICATIONS

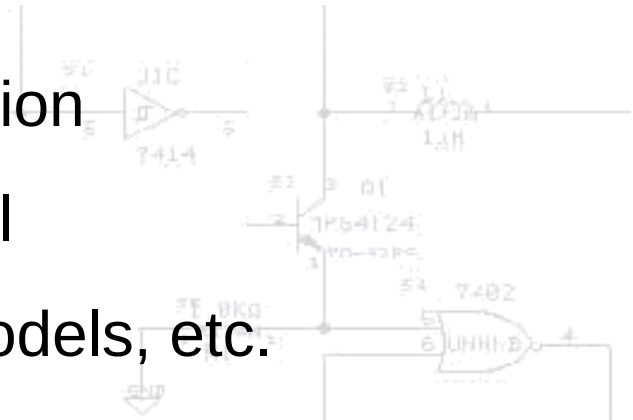
CA Duties

Defines policies for certificates

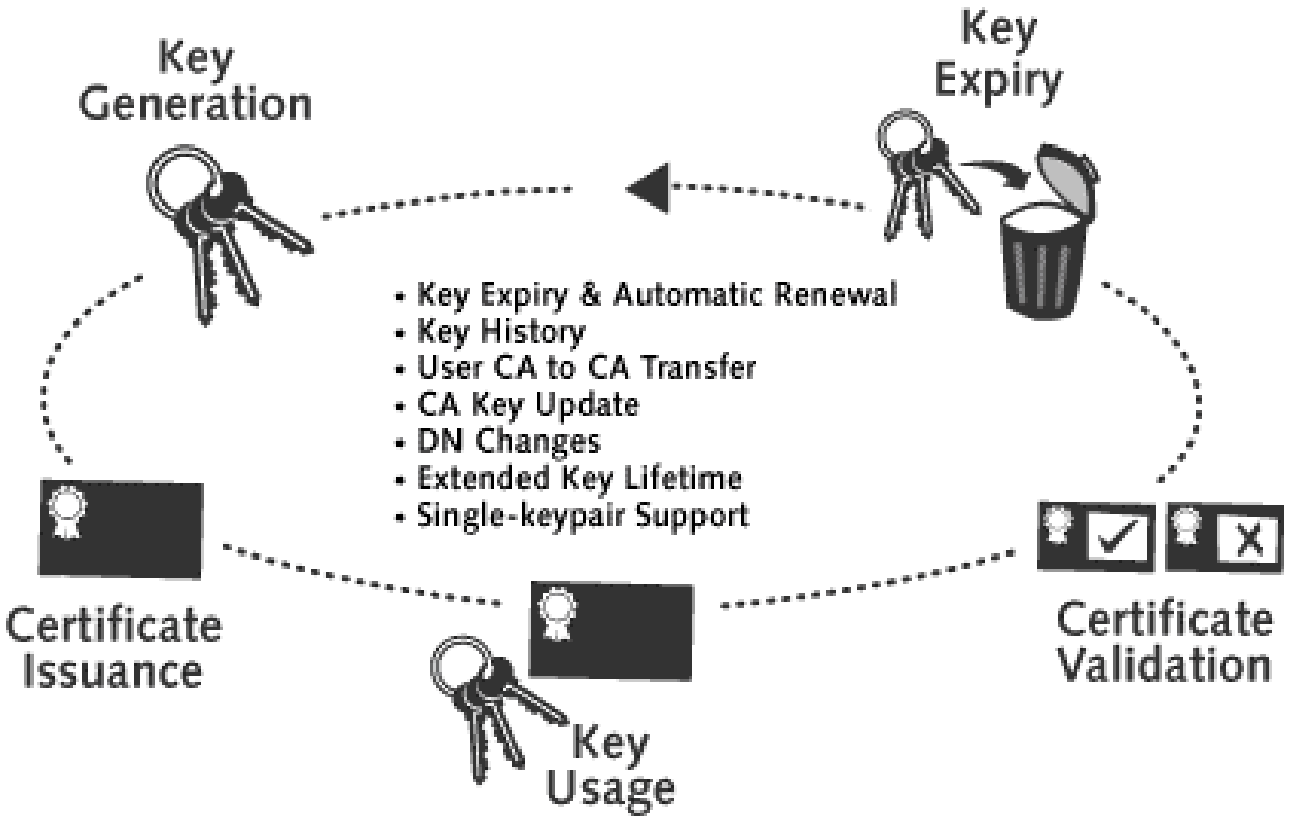
- Issuing
- Revocation
- Renewal
- Trust models, etc.

May issue different “classes” of certificates

- Permanent, contractor, temporary
- Employee, customer, partner



Certificate life cycle



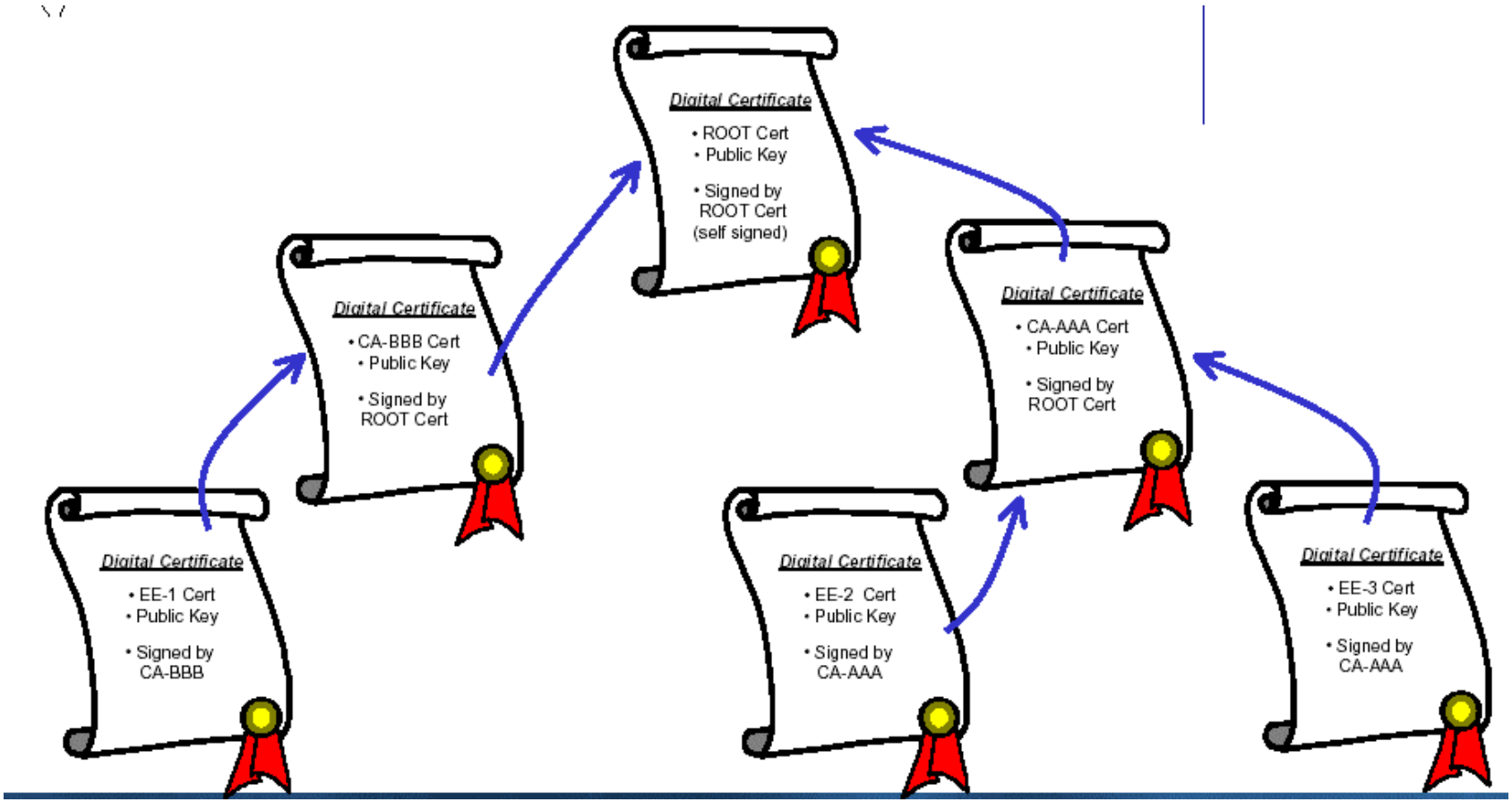
CA's as Trusted Third parties

When a new CA is established, its identity must be verified by having its public key signed by a higher authority.

This is the PEM model described in "Privacy Enhancement for Internet Electronic Mail, PART II Certified-Based Key Management" RFC-1422

Such requirement would create a hierarchy as shown in the next slide

CA Hierarchy



Steps to obtain a Digital Certificate

You submit a request to a CA, www.verisign.com

You provide personal information as part of the request.

A public/private key pair is also generated so that the public key becomes part of the certificate.

The certificate request is then forwarded to the CA in the form of PKCS #7 formatted information set.

CA validates the personal info (thru RA) and issues and digitally signs an X.509 formatted digital certificate.

The certificate is made public to the audience within PKI. Normally it is stored in a directory service (LDAP compliant)

Step by Step Verisign secure Server ID

•The U.S. Department of Commerce requires your company to qualify before buying the 128-bit SSL encryption

•**Install Web Server Software**

•U.S. software vendor properly classified by theU.S. Department of Commerce, including:

•• Apache-SSL

•• BEA WebLogic

•• C2Net Apache Stronghold

•• Compaq/Tandem iTP Webserver

•• Covalent Raven

•• Hewlett Packard Virtual Vault (with Netscape Enterprise)

U.S Application Server Software- Classified by Dept of Commerce

•• Apache-SSL
•• BEA WebLogic
•• C2Net Apache Stronghold
•• Compaq/Tandem iTP Webserver
•• Covalent Raven
•• Hewlett Packard Virtual Vault (with Netscape Enterprise)
•• IBM http Server/Webphone 1.3.3.1 and 1.3.6
•• iPlanet Servers
•• Lotus Domino 4.6.2 and later
•• Microsoft IIS 3.0 and later
•• Mod-SSL
•• Nanoteq Netseq server
•• Netscape Suite Spot servers, 3.0 or later, including Netscape
• Enterprise 3.0+ and Netscape Proxy Server 3.0 or later, 2.0
•• O'Reilly WebSite Pro v.2.5 and up
•• Red Hat Professional 6.1
•• Zeus

Step By Step Continued

- **Register your domain name**
- **Confirm firewall configuration**
- **Prepare payment**
- **Review legal agreement**
- **Gather proof of right documents**
- **Generate Certificate Signing Request**
- **Submit the Certificate Signing Request (CSR)**
- **to VeriSign**

REALSOFT
ADVANCED APPLICATIONS

How to Use the Digital Certificate

To participate in a transaction within the PKI, you can present the certificate to the other party.

The other party may actually retrieve the certificate from a directory service.

A challenge-response dialogue process can take place between you and the other party, so that the other party can confirm that you actually have the private key the corresponds to the public key found on the certificate.

The party can also validate the digital signature of the certificate to confirm the identity of the CA.

SSL is an http secure protocol that allows you to access and confirm the identity of a WEB SERVER and uses the above steps

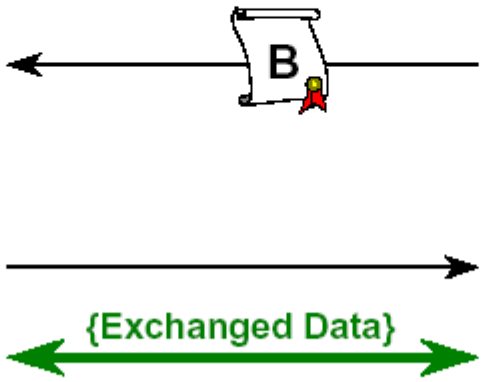
SSL secure sockets layer

Primarily used for Web Server Authentication
Invoked by using HTTPS and not HHTP

Which port / protocol

- **A** Connects to **B**
- **A** verifies signature on **B**'s certificate
- **A** generates Secret Session Key
- **A** uses **B**'s public key to encrypt Secret Session Key

- **B** sends copy of its certificate to **A**
- **B** uses its private key to decrypt Secret Session Key



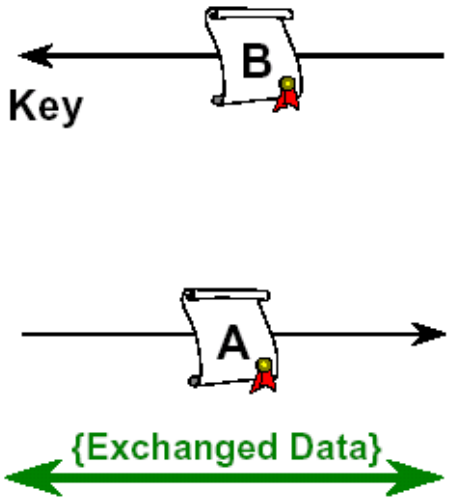
A and **B** use SSL Session Key to encrypt all data exchanged

SSL secure sockets layer Client side

Browser (**A**)

Secure Web Server (**B**)

- **A** Connects to **B**
- **A** verifies signature on **B**'s certificate
- **A** generates Secret Session Key
- **A** uses **B**'s public key to encrypt Secret Session Key
- Browser asks **A** to select a certificate to access **B**
- **A** sends encrypted Secret Session Key & **A**'s certificate to **B**



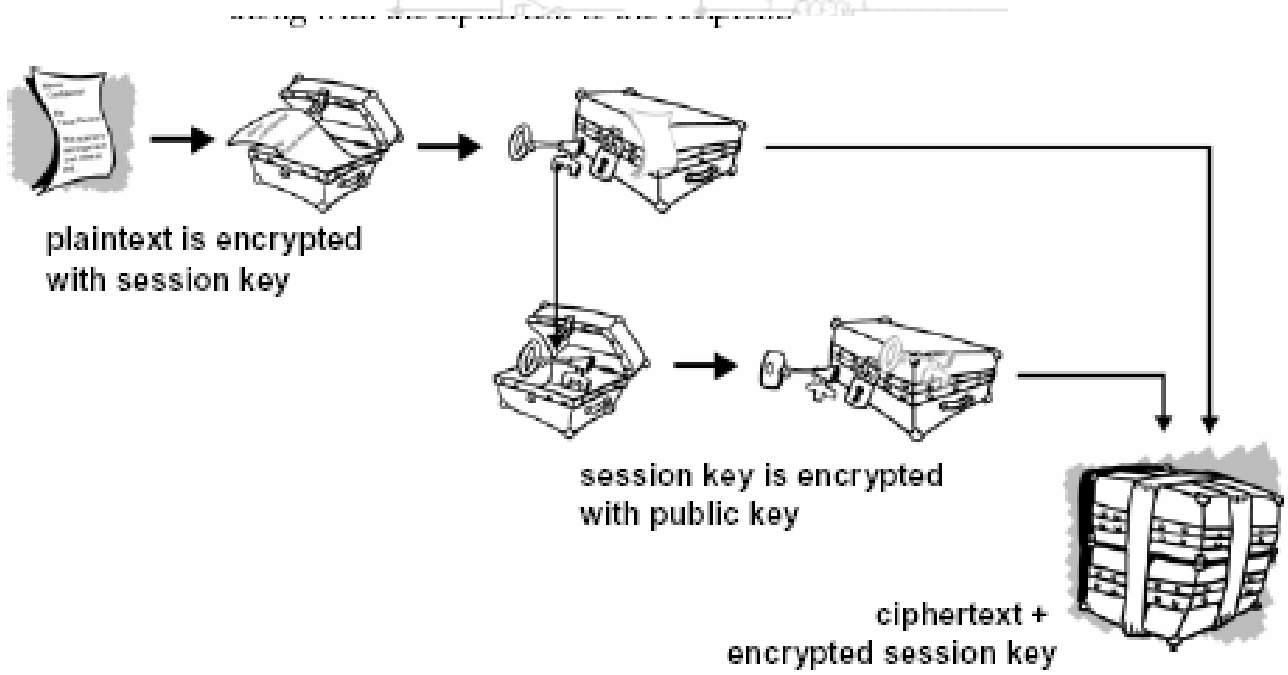
- **B** sends copy of its certificate to **A**, indicating that client authentication is enabled
- **B** verifies signature on **A**'s certificate
- **B** uses its private key to decrypt Secret Session Key

A and B use SSL Session Key to encrypt all data exchanged

Exchanging Session Key -SSL

Part of SSL (HTTPS PROTOCOL)

The idea is to use the faster symmetric-key technology for encryption, but to distribute the symmetric key utilizing public key technique



Directories -- LDAP

If a party with PKI wishes to initiate a contact with you, it needs to access your individual public key through your digital certificate.

CA maintains all certificates in a network directory services (A sort of a database).

The most common form of the network directory service is an X.500 compliant directory SERVER.

To access X.500 directory services a protocol that runs over TCP, called LightWeight Directory Access Protocol (LDAP) has been developed.

Windows 2000 includes LDAP compliant service called Active Directory; Oracle supplies it own LDAP called Oracle Internet Directory (OID).

Windows 2000 and LDAP

- Microsoft implementation of LDAP is called Active Directory.
- Its includes user account (username, password)
- Can include PKI certificates
- Can include Certification Revocation List (CRL) for invalidated certificates (Before their normal expiration time)
- Can include Access Control List (ACL)
- Applications can access the Active directory across the network using LDAP

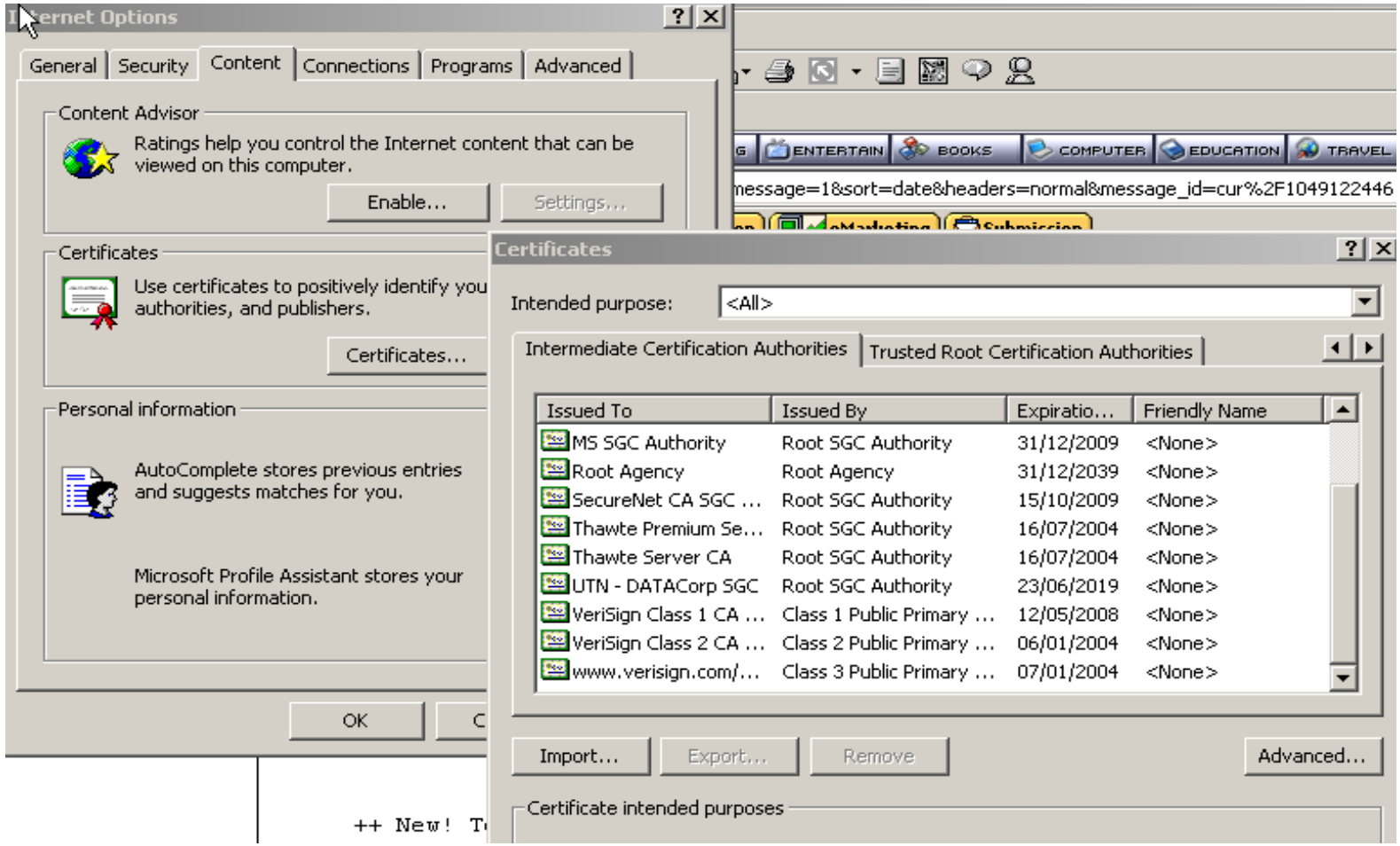
Oracle and LDAP

- **Oracle implementation of an LDAP compliant directory is called OID (Oracle Internet Directory).**
- **It is now part of Oracle Internet Application Server (IAS9i) middle tier infrastructure component.**
- **It is used to support all of the functionality used by Microsoft Active Directory explained in the previous slide.**
- **It is also used to centralize Usernames and passwords across multiple applications.**

Oracle and Single Sign On (SSO)

- Single Sign On is a security feature that centralizes you login information in a single active directory
- A SSO components allows you to connect to all of your application with a password entered only once.
- You login to the SSO server which then manages the connection to the application
- The application can be a database application, a mail etc ..

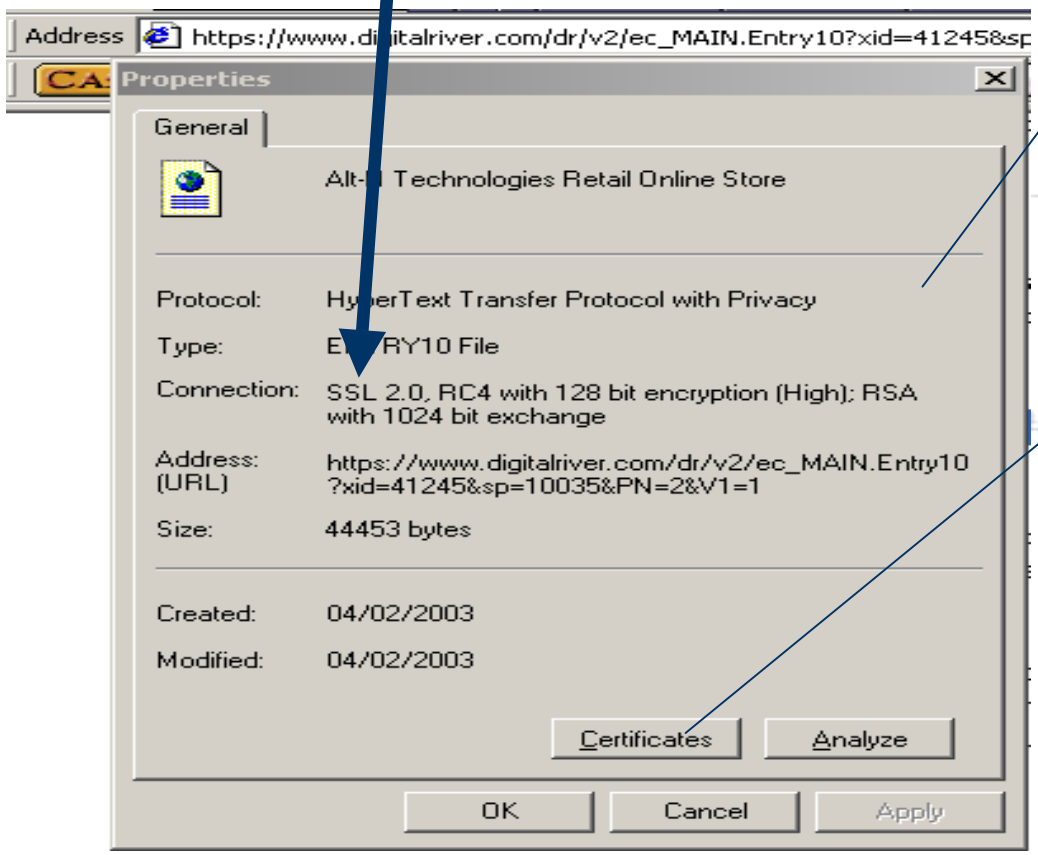
CA's supported by MS Explorer



REALSOFT
ADVANCED APPLICATIONS

Verify WEB Site Certificate on MS Explorer – www.digitalriver.com

Note: https:// and not http

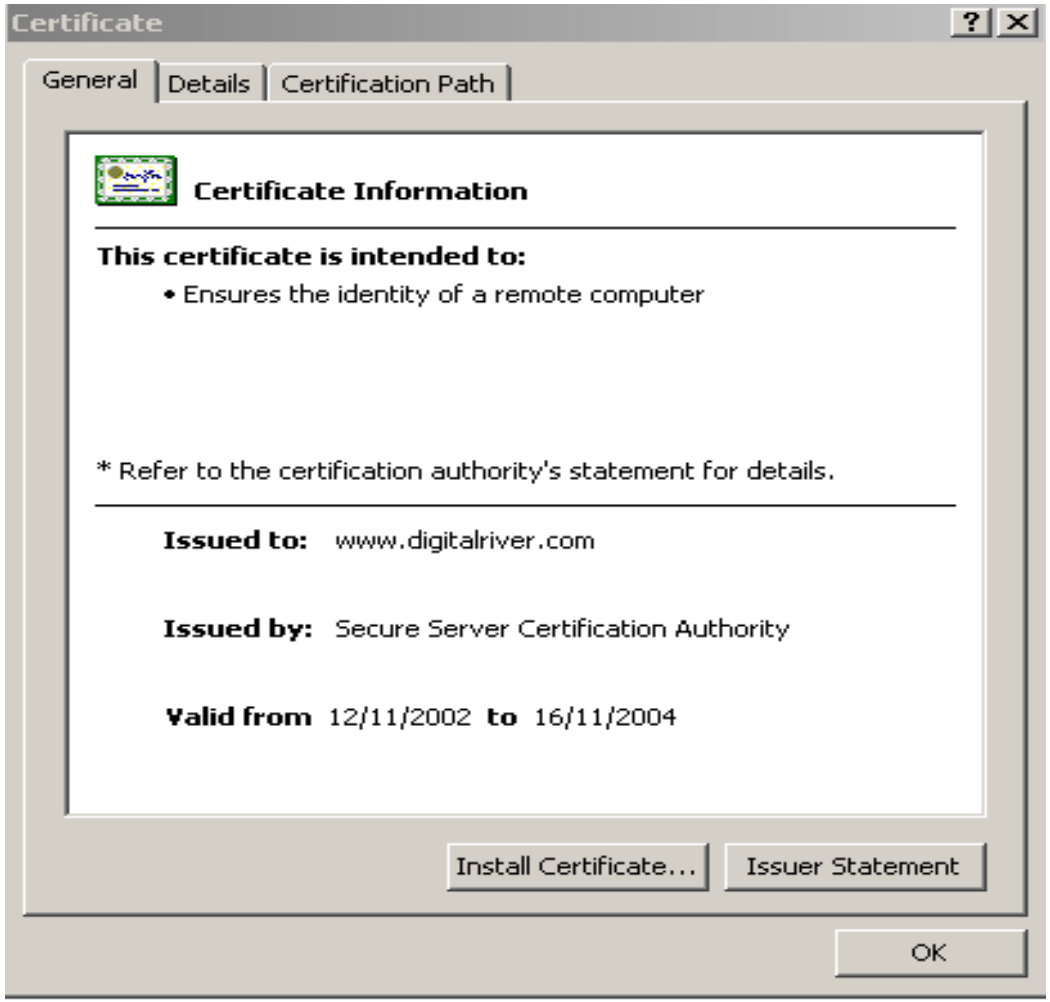


Use Right mouse click → Properties

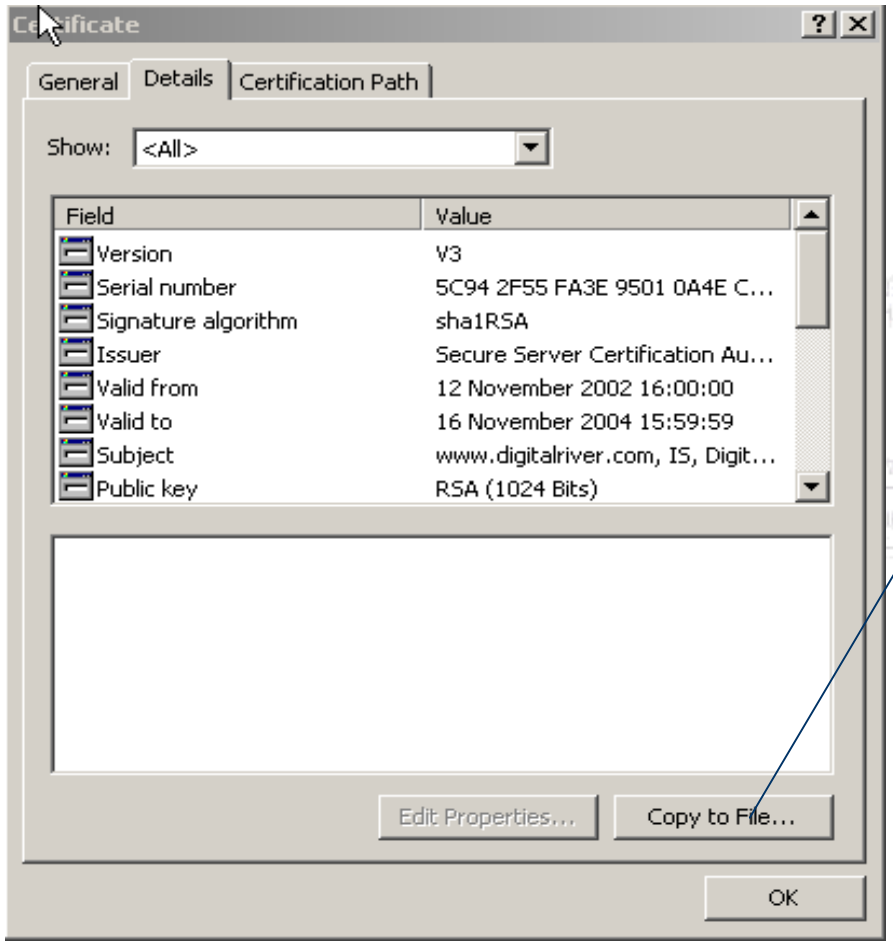
Press the Certificate s button

REALSOFT ADVANCED APPLICATIONS

View the certificate General Info of a www.digitalriver.com

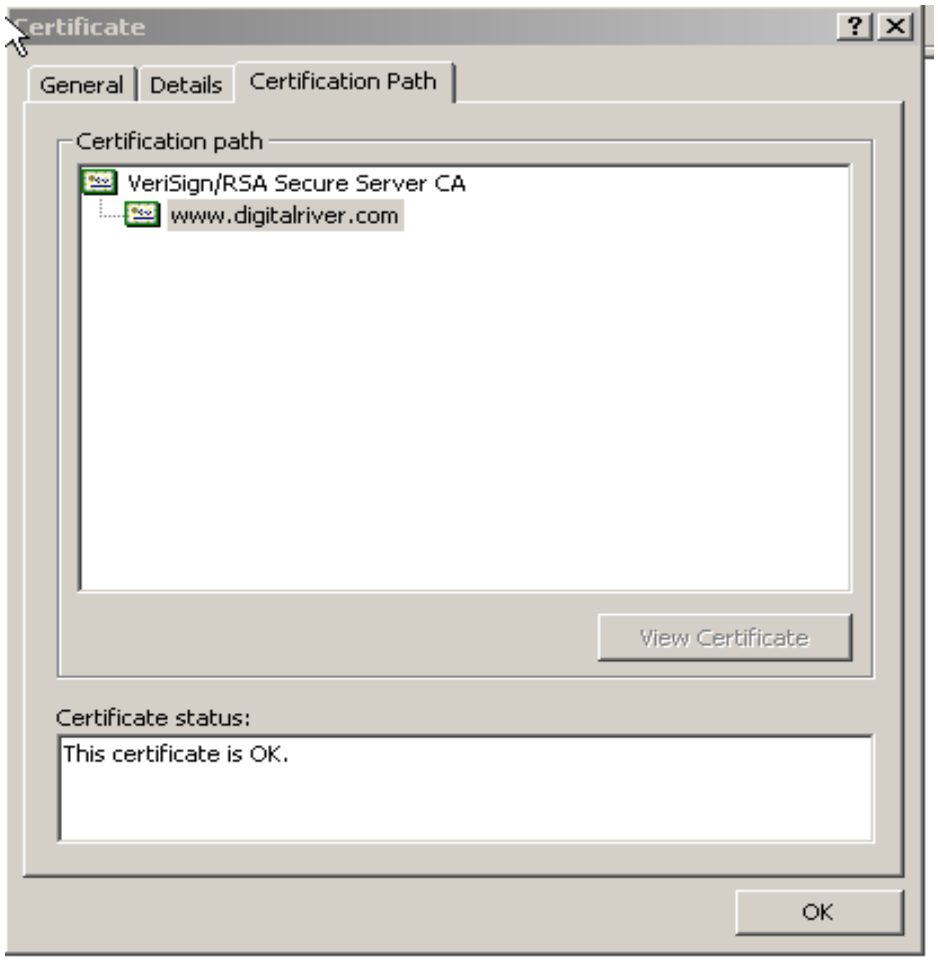


View the certificate Detail Info of a www.digitalriver.com



Note that you can copy it to a file

Certification Path information



Executable programs signing

Also known as code signing

Technique for signing executables with digital signature

Meant to provide a system for TRUSTING downloaded code and reducing the impact of malicious programs, including viruses and Trojan horses.

Two things are added to the code

A digital signature (The supplier private key)

A digital certificate with the supplier corresponding public key signed by an approved authority.

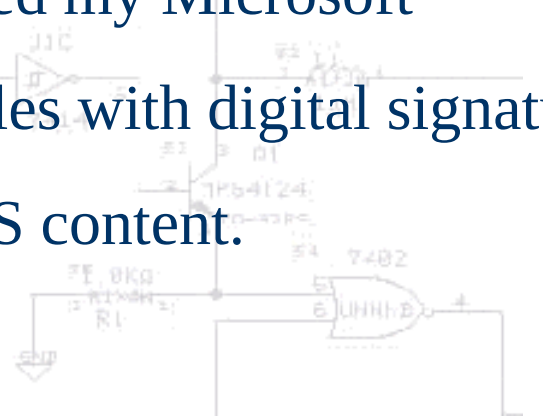
Code Signing today

Several proposal for code signing

Authenticode, developed my Microsoft

JAR, essentially ZIP files with digital signature

Extensions for the PICS content.



There are no U.S export controls on signed application, on programs for verifying signed applications, or on the public keys used to validate signed applications

THANK YOU AMERICA!!!!!!

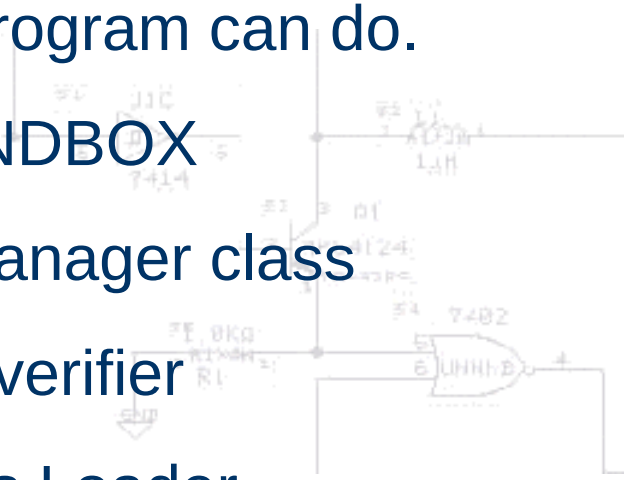
REALSOFT
ADVANCED APPLICATIONS

Signed Code is not SAFE CODE

- Does not provide users with a safe environment where they can run their programs
- Instead, code signing is intended to provide users with an *AUDIT TRAIL*.
- If a signed programs proves to be malicious, you should trail its originator.
- Signed Code can by hijacked

JAVA Applets Security

- Java employs a variety of techniques to limit what a downloaded program can do.
  - JAVA SANDBOX
  - SecurityManager class
  - Bytecode verifier
  - Java Class Loader



JAVA SANDBOX

- The Term is introduced by SUN Microsystems.
- Java programs are not allowed to directly manipulate a computer's hardware or making direct calls to the computers OS.
- Instead, Java programs are run on a virtual computer inside a restricted Virtual Space.

SecurityManager Class

All JAVA programs WERE not allowed

- To send information over the network.
- To read or write from the users hard disk
- To manipulate the computer input/output devices.

While running inside the sandbox, you can communicate with the outside world by calling the SecurityManager Class, designed to be called before any dangerous operation

Class loader

- To prevent a malicious programmer from disabling the Standard SecurityManager from within the program.
- Class loader examines classes to make sure that they do not violate the runtime system.

Bytecode Verifier

- Supposed to ensure that the bytecode that is downloaded could only have been created by compiling a valid java program.

- There are many problems with the JAVA security approach. For more info check the following book

Web Security and Commerce –

ISBN 1-56592-269-7 Garfinkel and Spafford -- Java Security Problems pp 50-54

Cookies

- A block of ASCII TEXT.
- Passed by Web Server into a user's Browser session.
- Cookies are kept in the web browser's memory.
- If a Cookie is of persistent type, it is also saved by the web browser
- Originally intended to make the Web server to track a client through multiple HTTP request.
- Is it a security problem?????

Client's Claimed Identity

•When you as a user login to an application, it is sometimes important to establish your identity as a client. Example, Trying to login to Arab Bank Internet Banking systme.

•It this discussion, authentication, authorization and access control are incorporated into the concept of identity

•Authentication is the process of validating the claimed identity of a user or a device (router, switch, firewall)

•Authorization is the process of granting access rights to a user, group or specified system.

•Access control is limiting the flow of information from resources to only authorized persons or system

Identity Technologies

- **S/KEY One-Time Password System**
- **Token Password authentication Scheme**
  - **Smart Card**
  - **Token Card**

S/Key Password protocol

Request for Comment

- Released by Bellcore and defined by RFC 1769
- A client/Server based protocol.
- Fights against somebody sniffing (eavesdropping) your password over the network.
- Based on MD4 MD5 scheme
- Password is hashed multiple time during transmission based on iteration count that specifies how many times to apply the hash function

Token based authentication

- **Requires the use of a special card**
- **Based on one of the two mechanism:-**
  - **Challenge – Response**
  - **Time – Synchronous**

Challenge Response

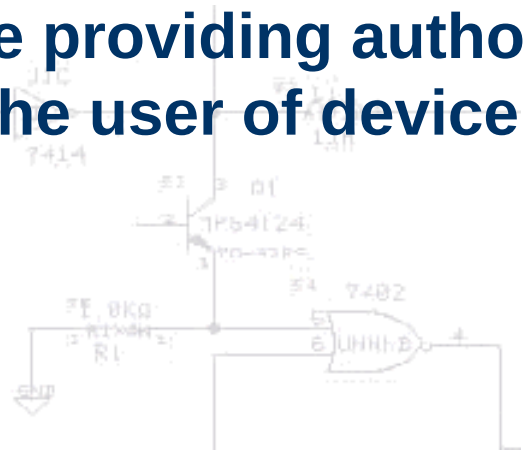
- The authentication Server prompts the user of an ID
- The user provides the ID to the server, which issues a challenge random number.
- The User enters this Random Number into a Token, which encrypts the challenge number with user's encryption key and displays a response
- The user types this response.
- The server has got a copy of the users key and can calculate what the response should be.

Time -Synchronous

- An algorithm runs on both the token and the authentication Server.
- The algorithm generates identical number on both the token and server that change over time.
- Such generated numbers act as a password.
- It is one time password, because the next login, the token generate a different number and the server expects that new number to allow access

Protocols Using Authentication mechanisms

- **These are protocols that require authentication verification before providing authorization and access rights to the user of device**
  - **TACACS+**
  - **RADIUS**
  - **Kerberos**
  - **DCE**
  - **FORTEZZA**



TACACS+

- Latest generation to TACACS, which is a simple UDP based Access Control Protocol
- CISCO has enhanced TACACS server times
- TACACS: Combines authentication and authorization
- XTACACS: Separated authentication , authorization and accounting
- TACACS+ with extended attribute control for accounting (Uses TCP and Port 49).
- At one time TACACS was implemented by GLOBAL ONE for authentication, authorization and accounting of its internet Dialup users. (maybe still one).
- TACACS Client is Normally a NAS (Network Access Server) and the Server is a software service

RADIUS

- Remote Address Dial-In User Service (RADIUS).
- Developed by Livingston Enterprise INC.
- Authentication, authorization and accounting.
- An ISP might use RADIUS access control and accounting software to meet special security and billing needs.
- RADIUS client is typically NAS and its server is usually a UNIX Process or NT service.
- FIRSTNET (Now part of BATELCO JORDAN) used RADIUS for its authentication, authorization and accounting, It was integrated with an ORACLE based Billing Software using ODBC connectivity developed by PALCO / REALSOFT -- The product is now dead

ACCESS CONTROL

What can be done to keep intruders out of a network?

The most common way is to use passwords and account numbers for logging on to a server or host, thus authenticating the user and authorizing access. (preferably encrypted to prevent sniffing)

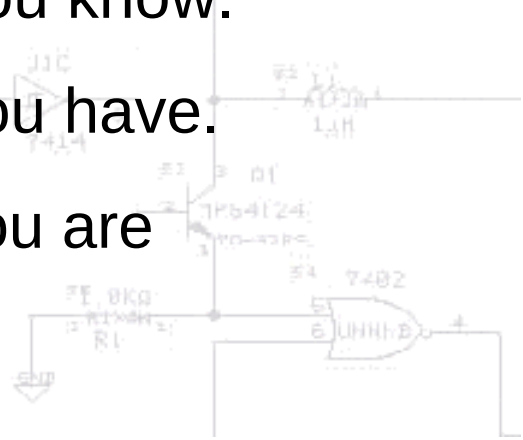
Another method to authenticate entities is to utilize a challenge/response sequence. For example:

1. **User-to-Card Authentication with a PIN code (or biometric). The user inputs his or her PIN or biometric and this is checked against the one stored on the card. This is very secure local transaction between the card and the user.**
2. **Card-to-Server Authentication. The server generates a random number as a "challenge" and sends it to the card. The challenge is encrypted by the card (using the private key on the card), and it is sent back to the server. The server decrypts it and checks the result against the original challenge. If they match, the card has been authenticated.**

Strong Authentication

Also called “non-key” authentication

- Something you know.
- Something you have.
- Something you are



Password,

Biometrics.

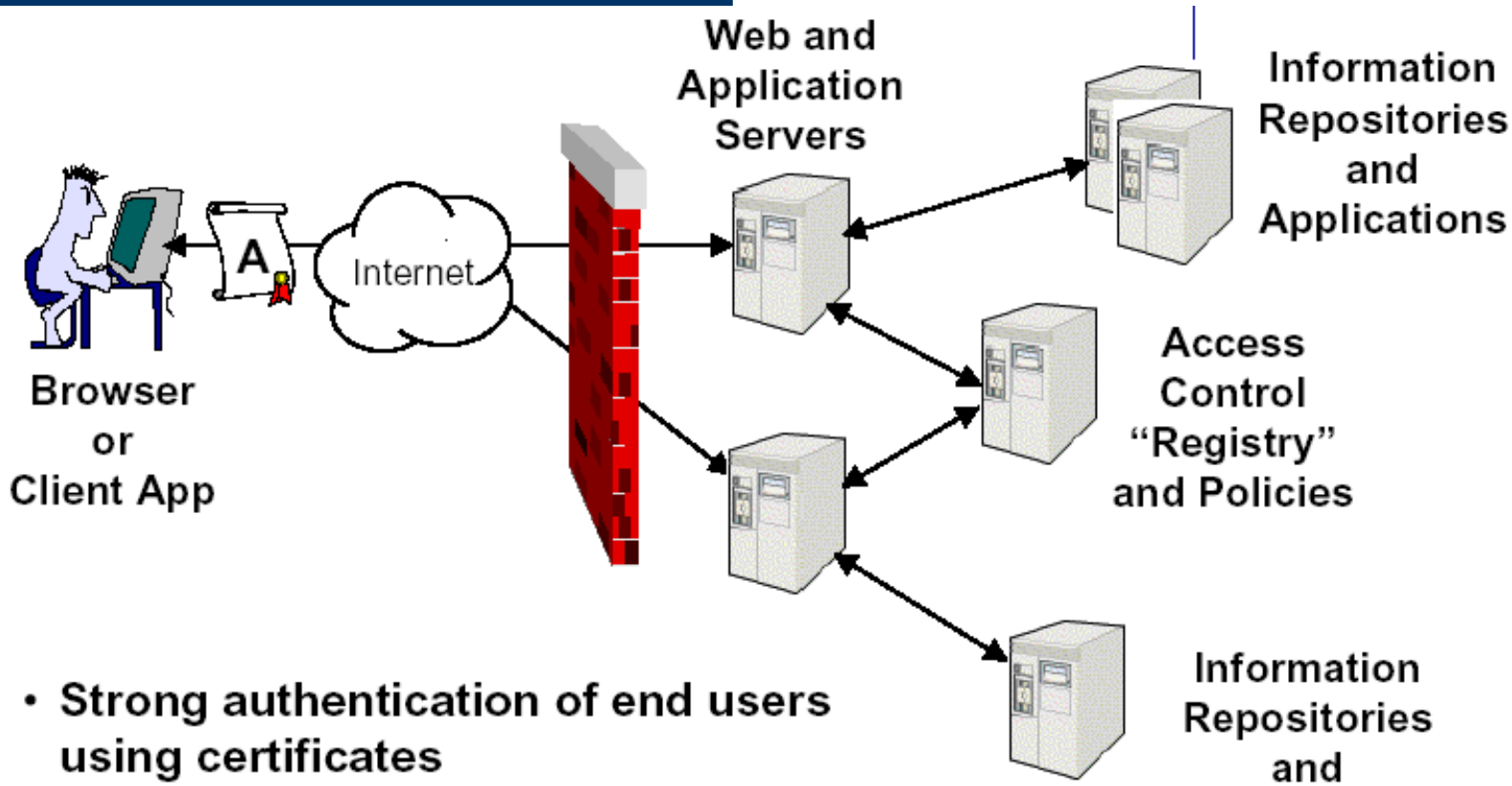
Smart card: inserted into reader (can provide one-time passwords, secret keys)

Token : no additional hardware needed

Biometrics

Technology	Secure	Easy to use	Compact	Low power	Cost effective
Finger print	5	5	4	5	4
Voice	2	4	5	5	5
Face	2	3	3	2	4
Hand	3	3	2	4	2
Signature	4	2	2	5	4
DNA	5+	1	1	1	1
Retina	5	1	3	3	3
Bone	4	1	1	1	1

Access Control and Firewalls

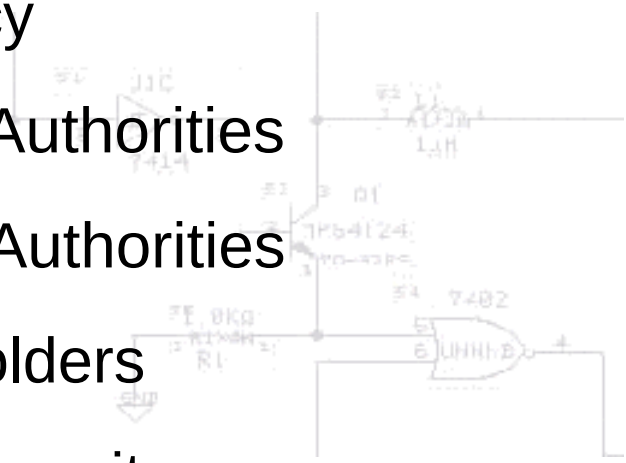


- Strong authentication of end users using certificates
- Fine grained access control
- "Single Sign On"

PKI revisited

Public Key Infrastructure PKI components are:

- Security Policy
- Certification Authorities
- Registration Authorities
- Certificate Holders
- Certificate Repository
- Validation Server



Smart Card and Security

Formal PKI Definitions

Security Policy defines an organization s direction on information security as well as the processes and principles for the use of cryptography.

Certification Authorities (CA) issue digital certificates to valid applicants, schedules expiry date for certificates and revokes them when the validity period expires.

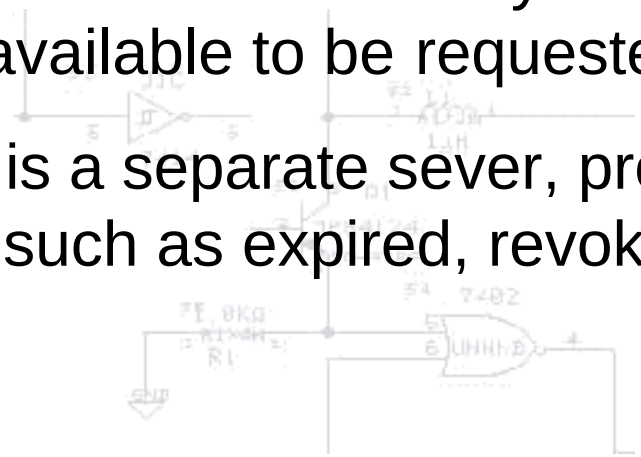
Registration Authorities (RA) provide the interface between the user and CA. It verifies the credentials of applicants and passes the valid requests to the CA.

Certificate Holders are subjects or end-entities which get the certificates from CA.

Formal Definitions (Cont'd)

Certificate Repository is the warehouse of PKI, storing and distributing certificate and entity information and making the data available to be requested.

Validation Server is a separate sever, providing certificate status, such as expired, revoked, etc.



PKI is secure

Many people perceive e-commerce to be insecure

The Fact is

•PKI services are more secure than exchanging private information over phone lines, thought the mail or even paying by credit card in person.

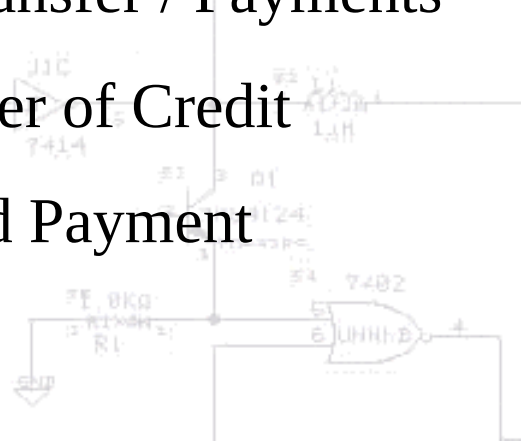
•Credit Card number can be stolen by a waiter while processing your bill, while public key algorithms are so secure than even millions of computers working in parallel could not possible break the code in a century.

Securing e-Business applications

- Online Auction Markets / Exchange Sites
- Online Procurement Solutions & Web Catalogues
- Corporate Purchasing
- Online Contracting
- Security solutions for traditional EDI
- Online delivery of intellectual products & professional services

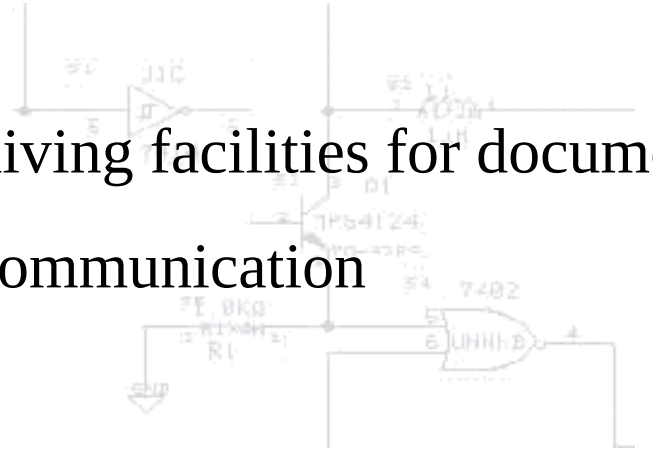
Security solutions for e-Banking

- Electronic Funds Transfer / Payments
- Trade Finance / Letter of Credit
- Bill Presentment and Payment
- Statement Delivery



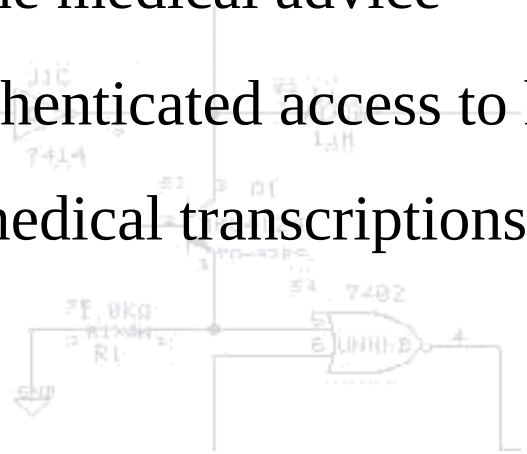
Securing E-office Applications

- Transformation to paperless office systems through digital signatures
- Encryption Archiving facilities for document storage
- Secure E-mail Communication



Securing Solutions for HealthCare

- Secure delivery of online medical advice
- Secure Storage and authenticated access to health records
- Privacy solutions for medical transcriptions



Security Solutions for Education

Security and authentication solutions for distance education and online examinations

- Security solutions for electronic certificates and credentials
- Online university application solutions
- Extended solutions for student identity along with smart cards

Securing E-government

- Overall security solutions for government documentation
- Online tax filing and payment solutions
- Online payment of public utility charges and government levies
- Online application and receipt of government approvals and clearances
- Secure web based notification system
- Secure tendering

Security Solutions for ERP and Supply Chain management

- Comprehensive security and authentication solution for the entire ERP / MRP Chain
- Signing capability for the database engine to record every alteration
- Secure transmission of information across the chain

Public Key Standards PKCS

Public Key Cryptography Standard(PKCS)

Some example of PKCS

PKCS#8 describes a syntax for private-key information.

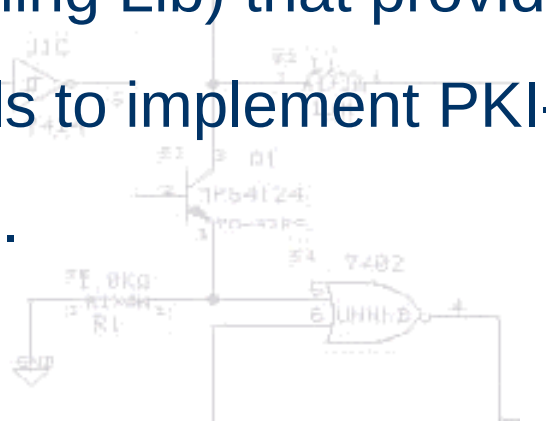
PKCS#9 defines selected attribute types for PKCS #7 digitally signed messages, and PKCS #8 private key information.

PKCS#10 describes a syntax for certification requests. A certification request consists of a distinguished name, a public key, and optionally a set of attributes

PKI compliant APIs

Baltimore KeyTool Pro 5.0

A Toolkit (Programming Lib) that provides you with all the necessary tools to implement PKI-compliant software applications.



REALSOFT
ADVANCED APPLICATIONS

Case Study – Implementing PKI in an Oracle Environment

REALSOFT
ADVANCED APPLICATIONS

Questions and Answers