INFORMATION SECURITY
Outline

- Information security challenges
- Cryptography
- Addressing information security challenges
- Digital certificates
INFORMATION SECURITY CHALLENGES
Secrecy/Privacy
An observer should not be able to access information
→ E.g. someone intercepting network packets
→ Particularly easy with wireless communications
Integrity

Data has not been tampered with

→ E.g. packets modified as they travel through network
Authentication

The author is the intended one

→ A user or system sending data pretending to be another one

→ Sometimes it includes integrity
Non Repudiation

The author cannot deny it

→ After having performed an operation a user states someone else did it on his/her behalf

→ E.g. on-line contract signing
→ Provides solutions to all the above
→ Literally: hidden writing
→ Deals with techniques and protocols
Encryption

- Information represented by a code
  - Coded version does not reveal the information
  - (Secret) techniques and parameters needed to reveal it
Computer Networks are an integral part of daily life.

Usually known

Usually secret

The longer the key, the stronger
Computer Networks are an integral part of daily life.

Symmetric key cryptography

Same as encryption key

Decryption

Same as encryption key

#$ˆ!@%^&^ 7jsdfk &*685 23*(&&*^*$J \*#(@HKJH? KFHDSAF<
Shared/Secret Key

→ Key must be shared securely

→ E.g. off-line
Requires pre-existing relation

If key is compromised on one party, no one can use it any longer
Asymmetric Key Cryptography

**RSA (2048 bit key)**

Computer Networks are an integral part of daily life.
Public Key Cryptography

- One of the two keys can be publicly distributed
  - Used for encryption
  - Public key
- Only owner of paired private key can decrypt
→ Private key never needs to be shared
→ Easier to keep safe
→ Keys are complementary
→ Repository for public keys
→ Associated to users
ADDRESSING INFORMATION SECURITY CHALLENGES
Secrecy/Privacy

Computer Networks are an integral part of daily life.
Symmetric and Asymmetric Cryptography

→ Asymmetric (d)encryption requires more computation power
→ Used for secure sharing of secret key
→ Shared secret to encrypt data
→ Periodically changed
Authentication

Computer Networks are an integral part of daily life.

A’s private key

A’s public key

A

B

Key repo
Digital Signature (Integrity+Authentication)

Computer Networks are an integral part of daily life.

Message digest

A’s private key

Signed document

Computer Networks are an integral part of daily life.
Computer Networks are an integral part of daily life.
Cryptographic Digest (Hash)

A’s private key

Electronic signature

Computer Networks are an integral part of daily life.

MD5 (128 bit digest)
SHA (160 bit digest)
What if the signer’s public key is not the signer’s

- An authentication problem
- Signature can solve it
DIGITAL CERTIFICATES

A.k.a. public-key certificates
What is it?
A key with a tag, both signed

But who is going to sign it?
Certification Authority

→ CA needs to verify owner’s identity before signing
  → E.g. show up in person with a piece of ID
→ Can be used to enforce non repudiation
**Keychain Access**

Click to lock the login keychain.

### Keychains
- **login**
- Micr...certificates
- System
- System Roots

### My Certificates

<table>
<thead>
<tr>
<th>Name</th>
<th>Kind</th>
<th>Expires</th>
<th>Keychain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mario Baldi</td>
<td>certificate</td>
<td>Jan 1, 2016 12:59:59 AM Central European Standard Time</td>
<td>login</td>
</tr>
<tr>
<td>Mario Baldi</td>
<td>private key</td>
<td>--</td>
<td>login</td>
</tr>
<tr>
<td><strong>Subject Name</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>--</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Country</strong></td>
<td>IT</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Politecnico di Torino</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
<td>Mario Baldi</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>User ID</strong></td>
<td>d002520</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Issuer Name</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Country</strong></td>
<td>IT</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Politecnico di Torino</td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
<td>Politecnico di Torino Certification Authority</td>
</tr>
</tbody>
</table>

| **Serial Number** | 1232 |
| **Version**       | 3 |

| **Signature Algorithm** | SHA-1 with RSA Encryption (1.2.840.113549.1.1.5) |
| **Parameters**         | none |

| **Not Valid Before**   | Friday, January 11, 2013 2:32:54 PM Central European Standard Time |
| **Not Valid After**    | Friday, January 1, 2016 12:59:59 AM Central European Standard Time |

<table>
<thead>
<tr>
<th><strong>Public Key Info</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Algorithm</strong></td>
<td>RSA Encryption (1.2.840.113549.1.1.1)</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>none</td>
</tr>
<tr>
<td><strong>Public Key</strong></td>
<td>256 bytes : CB B9 1C B6 63 D2 F8 7E ...</td>
</tr>
<tr>
<td><strong>Exponent</strong></td>
<td>65537</td>
</tr>
<tr>
<td><strong>Key Size</strong></td>
<td>2048 bits</td>
</tr>
<tr>
<td><strong>Key Usage</strong></td>
<td>Encrypt, Verify, Wrap, Derive</td>
</tr>
<tr>
<td><strong>Signature</strong></td>
<td>256 bytes : 96 2C 89 08 6C 82 77 89 ...</td>
</tr>
</tbody>
</table>
PKI: Public Key Infrastructure

→ Impractical to have
  → One CA
  → Multiple independent CAs

Certification Authority Hierarchy
Certificate Issuance

→ CA verifies owner’s legal identity
  → Possibly through Registration Authority
→ CA generates key pair
→ CA assembles and signs cert
→ Cert. published in repository
  → Contains public key
→ Owner is given private key
→ Owner is given root CA cert
Does the whole World trust one Root CA?

- Unfortunately not
- Several Root CAs

How do we get their certs?
Embedded in operating systems/browsers

We all trust software vendors!??!

(maybe just because we don’t know it)