Public Key Infrastructure (PKI)

MIH-CPP
PKI

• An infrastructure that uses public key or asymmetric cryptography involving the use of two keys:
  – a public-key, which may be known by anybody, and can be used to encrypt messages, and verify signatures
  – a related private-key, known only to the recipient, used to decrypt messages, and sign (create) signatures

• Infeasible to determine private key from public

• Is asymmetric because
  – two different keys
PKI Guarantees

• Supports:
  – encryption/decryption (provide confidentiality)
  – digital signatures (provide authentication)
  – key exchange (of session keys)

• Some algorithms are suitable for all uses, others are specific to one

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Encryption/Decryption</th>
<th>Digital Signature</th>
<th>Key Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Elliptic Curve</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Diffie-Hellman</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>DSS</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Confidentiality through PKC

Image Source: Cryptography and Network Security by William Stallings
Authentication through PKC

Image Source: Cryptography and Network Security by William Stallings
Hash Functions

- MD5 or SHA256
- Computationally infeasible to find data mapping to specific hash (one-way property)
- Computationally infeasible to find two data to same hash (collision-free property)

Image Source: Cryptography and Network Security by William Stallings
Hash Functions & Digital Signatures
(a) Obtaining certificates from CA

\[ C_A = E(PR_{\text{auth}}, [T_1 \| ID_A \| PU_a]) \]

\[ C_B = E(PR_{\text{auth}}, [T_2 \| ID_B \| PU_b]) \]

(b) Exchanging certificates

\[ (1) C_A \]  
\[ (2) C_B \]