Cryptography

Site information → CA → M

M → E → C → D → M

Encryption key → K_e
Decryption key → K_d

Forms of attack:
ciphertext-only
known-plaintext
chosen-plaintext

Forms of Cryptosystems

• Private Key:
  A single key is used for both encryption and decryption.
  Key distribution problem -a secure channel is needed to transmit the key before secure communication can take place over an unsecure channel.

• Public Key:
The encryption procedure (key) is public while the decryption procedure (key) is private.

Requirements:
1. For every message M, D(E(M)) = M
2. E and D can be efficiently applied to M
3. It is impractical to derive D from E.
Secure Communication in a Public Key System

Rivest-Shamir-Adelman (RSA) Method

Encryption Key for user Y
Decryption Key for user Y
RSA Method

1. Choose two large (100 digit) prime numbers, p and q, and set 
n = p \times q 

2. Choose any large integer, d, so that: 
GCD(d, (p-1) \times (q-1)) = 1 

3. Find e so that: 
e \times d = 1 \pmod{(p-1) \times (q-1)} 

Example:
1. p = 5, q = 11 and n = 55. 
   \((p-1) \times (q-1) = 4 \times 10 = 40\)

2. A valid d is 23 since \(GCD(40, 23) = 1\)

3. Then e = 7 since: 
   \(23 \times 7 = 161 \pmod{40} = 1\)

Authentication

Authentication Services:
digital signatures
interactive communication (client-server)
one-way communication (electronic mail)

Forms of Attack:
replay of messages
interference (inserting bogus messages)

Authentication Servers:
maintain a list of (user, key) pairs
securely distributes conversation keys
Digital Signatures (Public Key)

Requirements:
- unforgable and unique
  - receiver: knows that a message came from the sender
  - sender: cannot deny authorship
- message integrity
  - message signature unchangeable
    (e.g., cannot cut and paste a signature into a message)

Public Key System:
- sender, A: (E_A : public, D_A : private)
- receiver, B: (E_B : public, D_B : private)

sender(A) \rightarrow C = E_B (D_A (M)) \rightarrow receiver(B)
receiver(B) \rightarrow M = E_A (D_B (C)) \rightarrow M

Secure Communication (Public Key)

Handshaking

\begin{figure}
\centering
\begin{tikzpicture}
\node (A) at (0,0) {A};
\node (B) at (2,0) {B};
\draw[->] (A) -- node[above]{E_{PKB} (I_A, A)} (B);
\draw[->] (B) -- node[below]{E_{PKA} (I_A, I_B)} (A);
\draw[->] (B) -- node[below]{E_{PKB} (I_B)} (A);
\end{tikzpicture}
\end{figure}

I_A, I_B are "nonces"
nonces can be included in each subsequent message
Secure Communication (Public Key)

Obtaining a Public Key:

Suppose that A and B have not previously communicated. How does A securely obtain the public key of B?

An authentication server (AS) with a public key (PKAS) and a private, or secret, key (SKAS) is used as follows:

\[ \text{A} \rightarrow \text{AS}: (A, B) \]
\[ \text{AS} \rightarrow \text{A}: E_{SKAS} (PKB, B) \]

Note:

- The original message need not be encrypted
- A can decrypt the response from AS using PKAS
- A knows that the response can only have come from AS
- A knows that the response contains the key for B