### Cryptography

**Site Information**

E: C

K_e

Encryption key

D: M

K_d

Decryption key

**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

User X

M

E_Y (M) → C

D_Y (C) → M

User Z

### Rivest-Shamir-Adelman (RSA) Method

**RSA Method**

1. Choose two large (100 digits) prime numbers, p and q, and set 
   \( n = p \times q \)
2. Choose any large integer, d, so that:
   \( \text{GCD}(d, (p-1)(q-1)) = 1 \)
3. Find e so that:
   \( e \times d = 1 \pmod{(p-1)(q-1)} \)

**Example:**

1. \( p = 5, q = 11 \) and \( n = 55 \).
   \( (p-1)(q-1) = 4 \times 10 = 40 \)
2. A valid d is 23 since \( \text{GCD}(40, 23) = 1 \)
3. Then e = 7 since:
   \( 23 \times 7 = 161 \pmod{40} = 1 \)

User X

\( M \pmod{n} \rightarrow C \)

User Y

### 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:
- unforgeable 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: \( (E_A: \text{public}, D_A: \text{private}) \)
- receiver, B: \( (E_B: \text{public}, D_B: \text{private}) \)
- \( \text{sender(A)} - \rightarrow C = E_B(D_A(M)) \)
- \( \text{receiver(B)} - \rightarrow M = E_A(D_B(C)) \)

Secure Communication (Public Key)

Handshaking

\[ \begin{align*}
    & A \\
    & E_{SKA}(I_A, A) \\
    & E_{PKA}(I_A, B) \\
    & E_{PKB}(B) \\
    & B
\end{align*} \]

I_A, I_B are “nonces”
nonces can be included in each subsequent message

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:

A \( \rightarrow \) AS: \( (A, B) \)
AS \( \rightarrow \) A: \( E_{SKA}(PKB, B) \)

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

Secure Communication (Public Key)