

Cryptographic Security

Security Considerations

Factors:

- **reliance on unknown, vulnerable intermediaries (e.g., Internet routers)**
- **parties may have no personal or organizational relationship (e.g., e-commerce)**
- **use of automated surrogates (e.g., agents)**

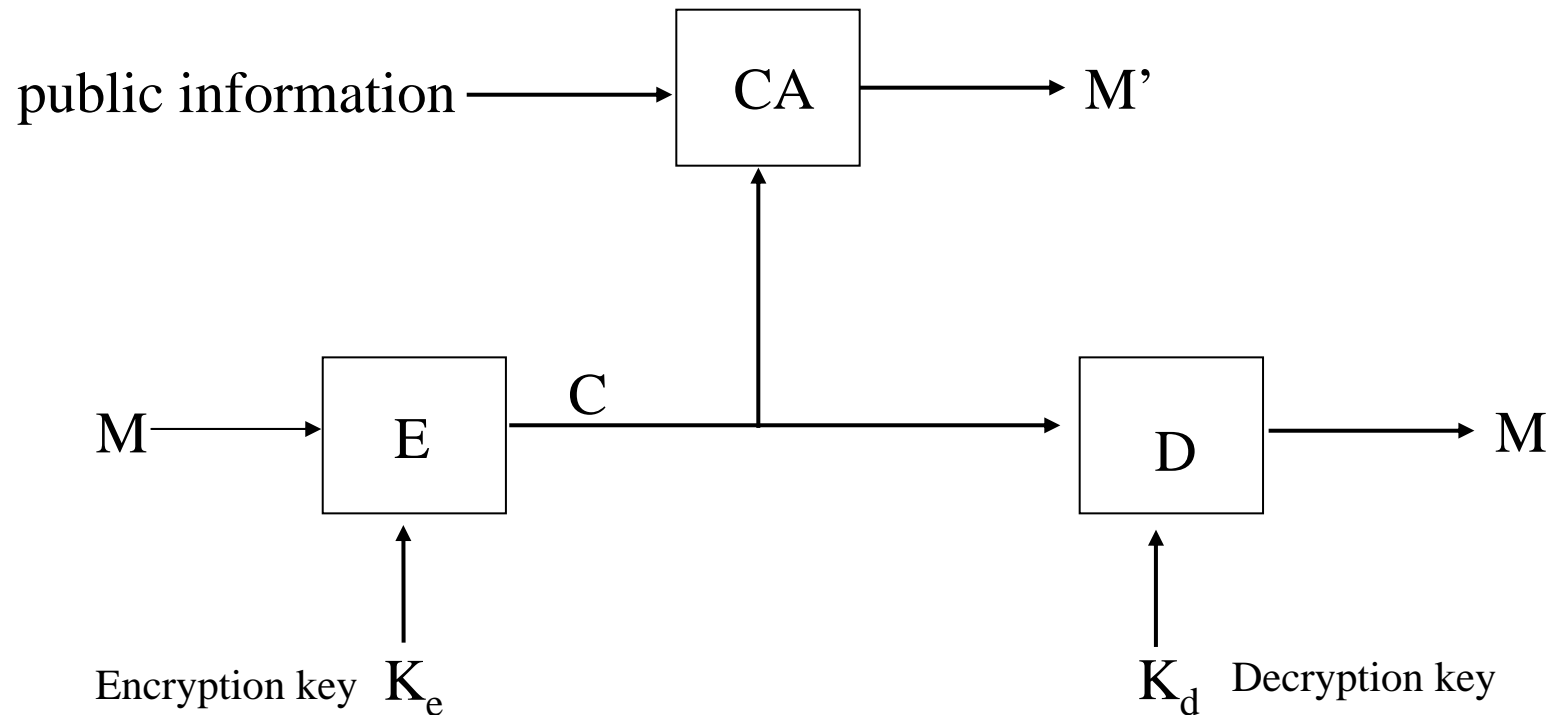
Goals:

- **privacy/confidentiality - information not disclosed to unauthorized entities**
- **integrity - information not altered deliberately or accidentally**
- **authentication - validation of identity of source of information**
- **non-repudiation - source of information can be objectively established**

Threats:

- **replay of messages**
- **interference (inserting bogus messages)**
- **corrupting messages**

Cryptography



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

Forms of Cryptosystems

- **Private Key (symmetric) :**

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 (asymmetric):**

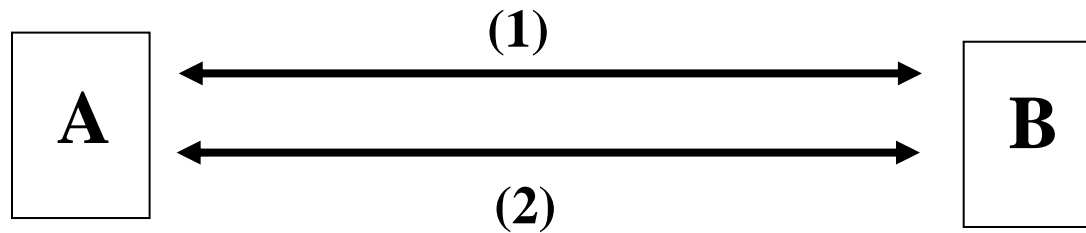
The encryption procedure (key) is public while the decryption procedure (key) is private.

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 .

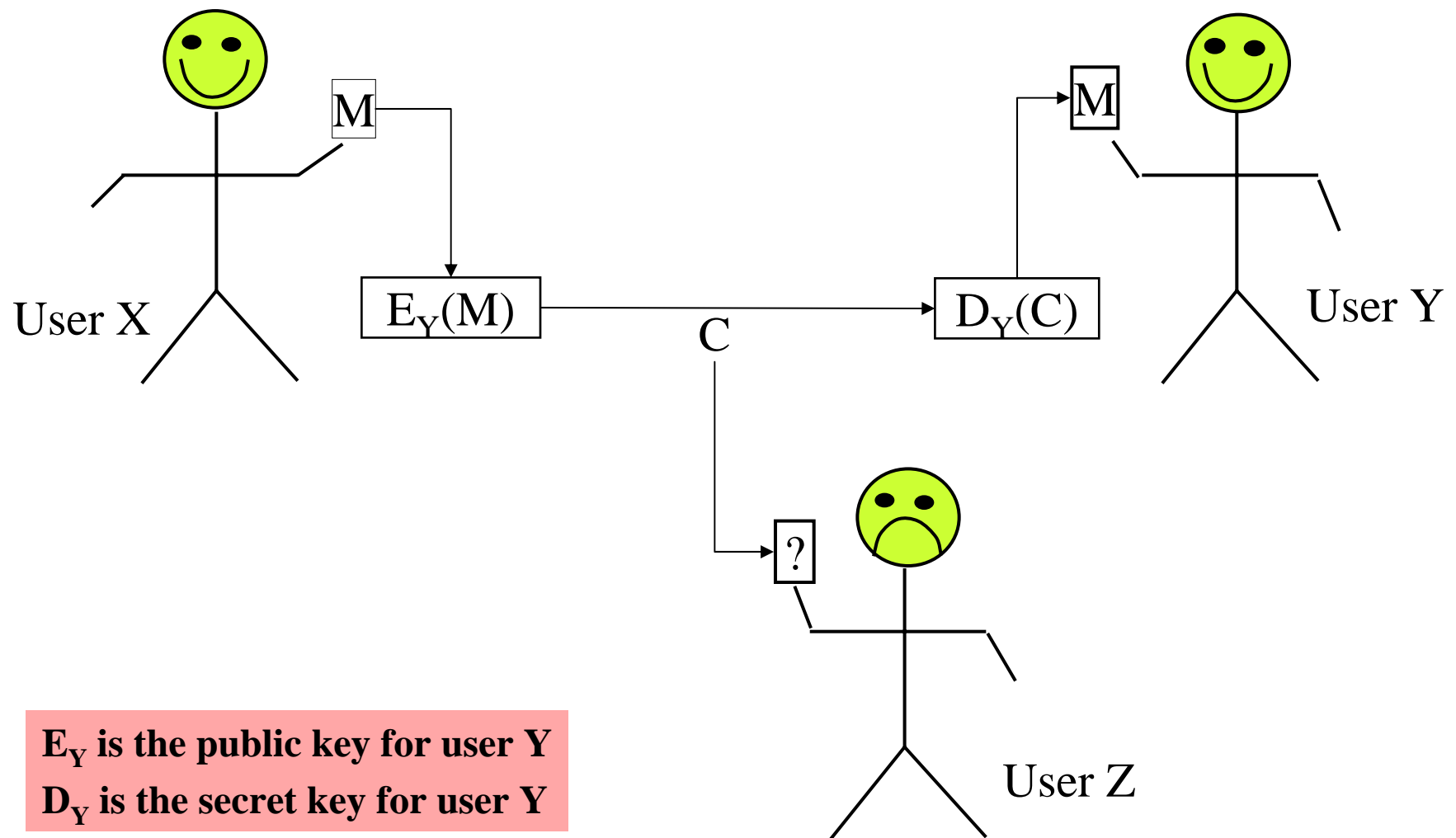
Combining Public/Private Key Systems

Public key encryption is more expensive than symmetric key encryption
For efficiency, combine the two approaches

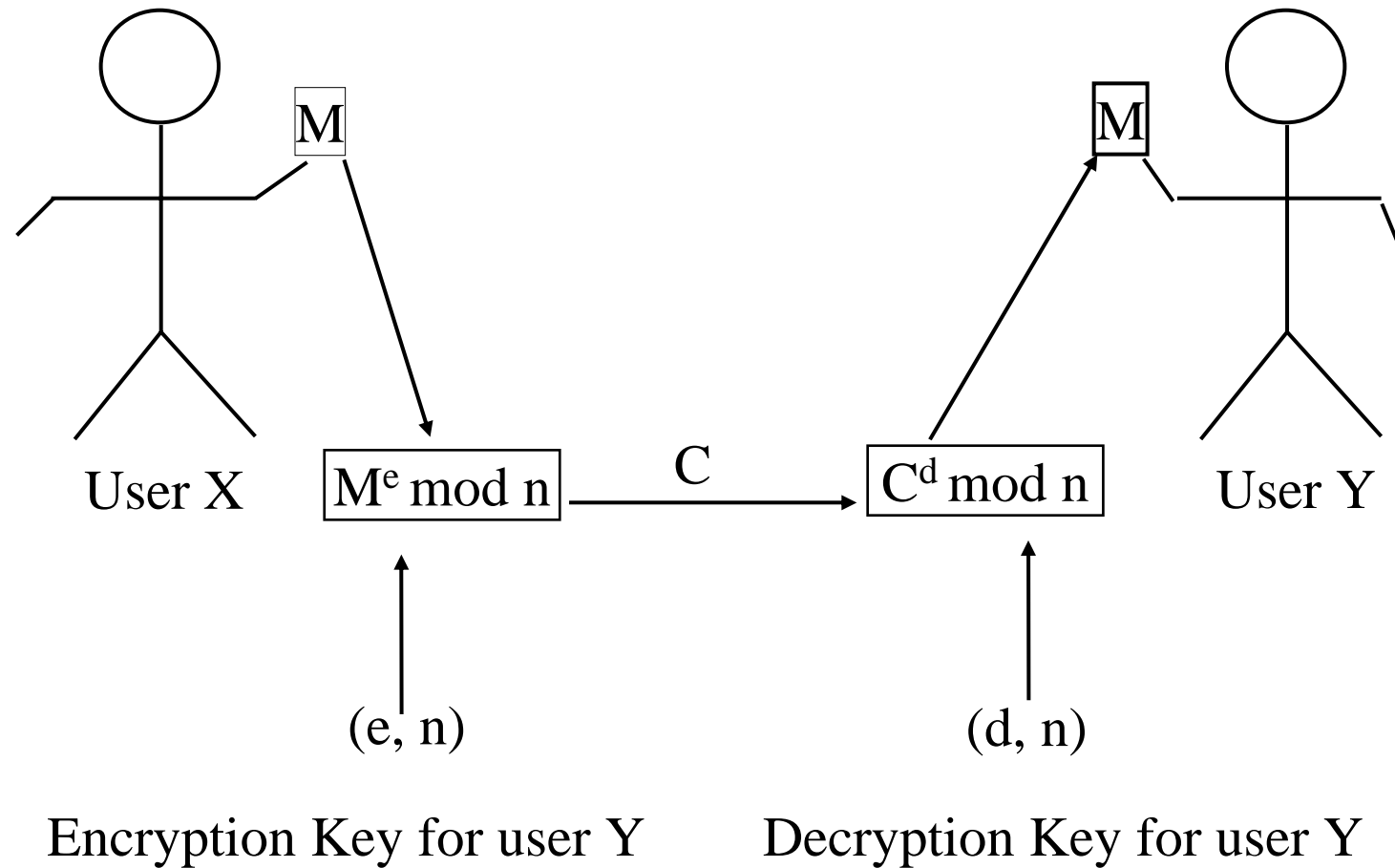


- (1) Use public key encryption for authentication; once authenticated, transfer a shared secret symmetric key**
- (2) Use symmetric key for encrypting subsequent data transmissions**

Secure Communication - Public Key System



Rivest-Shamir-Adelman (RSA) Method



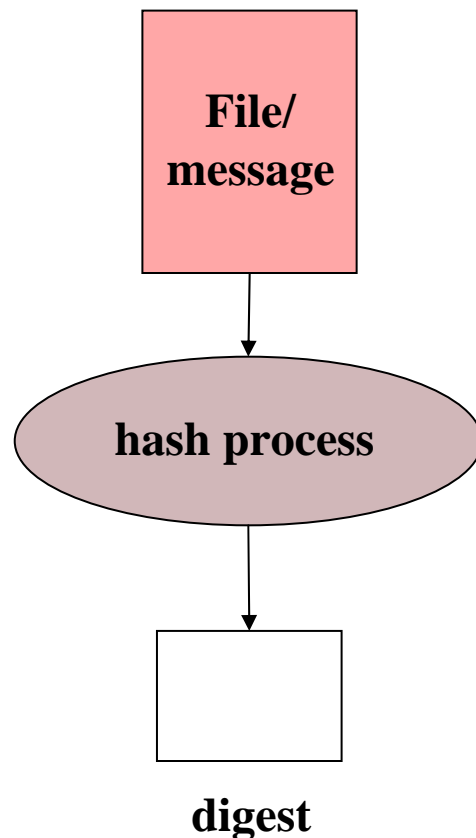
RSA Method

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: $\text{GCD}(d, ((p-1) \times (q-1))) = 1$
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 $\text{GCD}(40, 23) = 1$
3. Then $e = 7$ since:
 $23 \times 7 = 161 \pmod{40} = 1$

(Large) Document Integrity



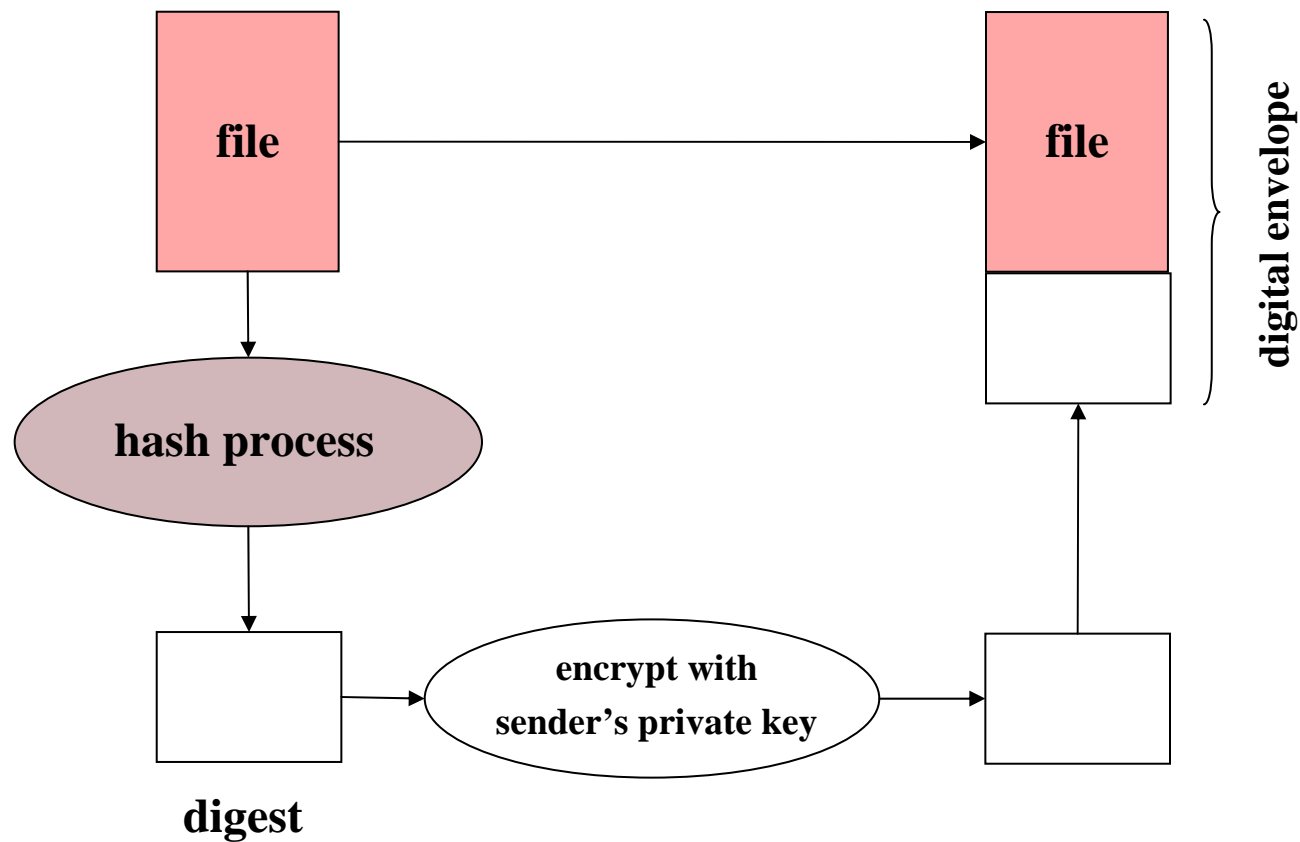
Digest properties:

- **fixed-length, condensation of the source**
- **efficient to compute**
- **irreversible - computationally infeasible for the original source to be reconstructed from the digest**
- **unique - difficult to find two different sources that map to the same digest (collision resistance)**

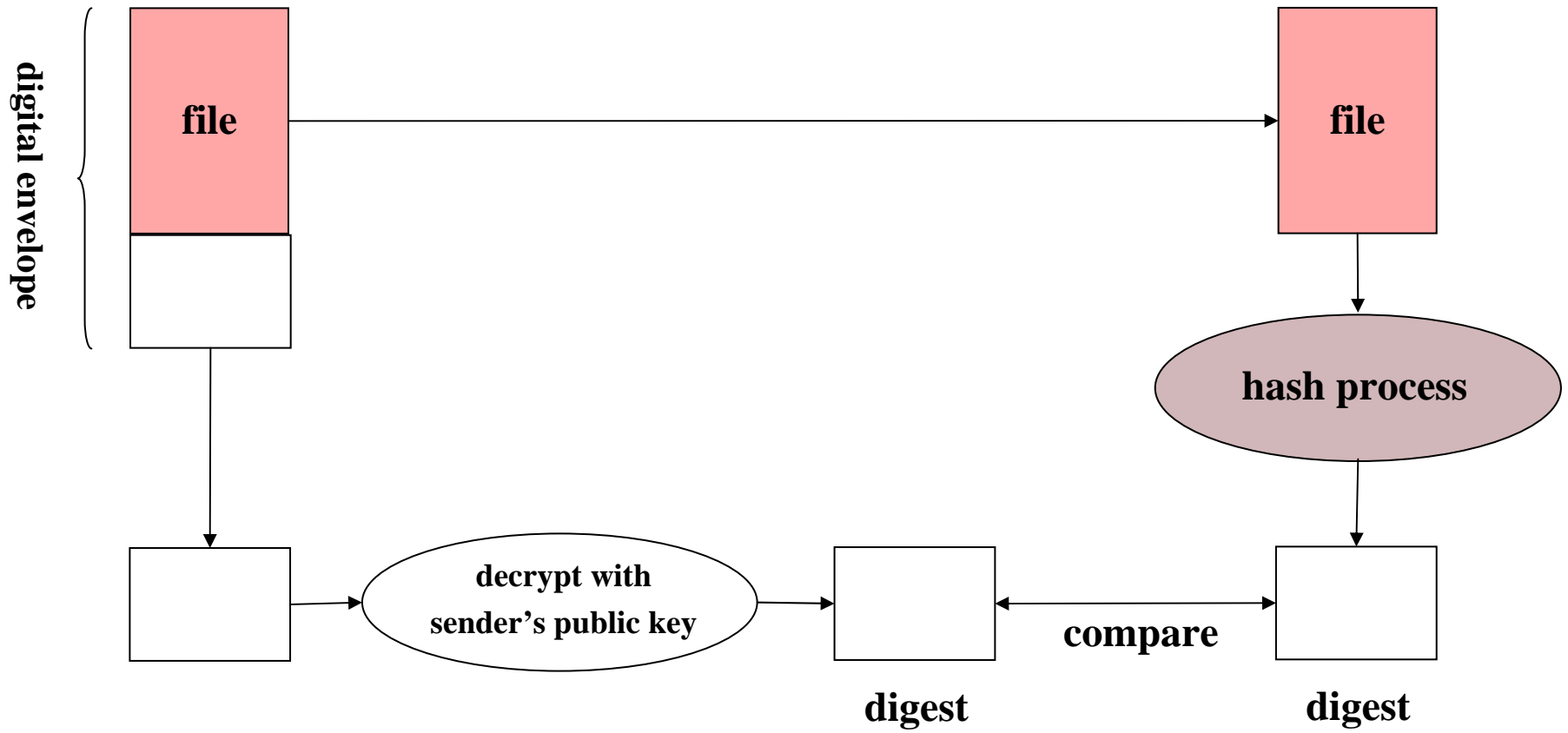
Also known as: fingerprint

Examples: MD5 (128 bits), SHA-1 (160 bits)

(Large) Document Integrity



Guaranteeing Integrity



Digital Signatures (Public Key)

Requirements:

unforgable and unique

receiver: knows that a message came from the sender (authenticity)

sender: cannot deny authorship(non-repudiation)

message integrity

sender & receiver: message contents preserved (integrity)

(e.g., cannot cut-and-paste a signature into a message)

Public Key System:

sender, A: (E_A : public, D_A : private)

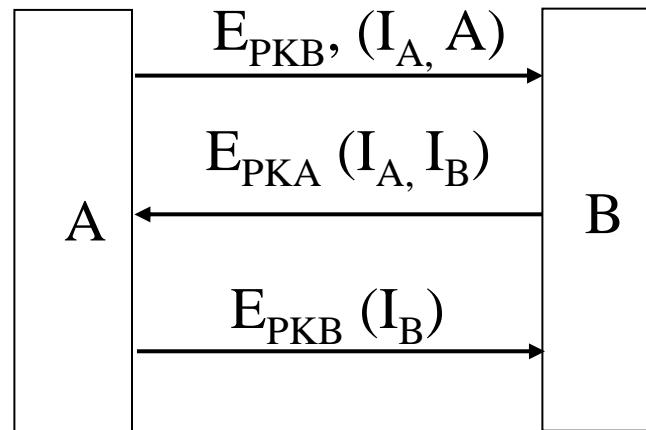
receiver, B: (E_B : public, D_B : private)

sender(A) ---- $C = E_B (D_A (M))$ ----> receiver(B)

receiver(B) -- $M = E_A (D_B (C))$ ----> M

Secure Communication (Public Key)

Handshaking



I_A, I_B are “nonces”

nonces can be included in each subsequent message

PKB: public key of B; PKA: public key of A;