Lecture 08 · SENG 41283 · Distributed and Cloud Computing

Security in Distributed Systems

Threats and Attacks · Cryptography · Authentication · Digital Signatures · Certificates · Firewalls

1. Introduction

Processes encapsulate resources; principals (users or processes) are authorised to operate on resources which must be protected against unauthorised access. Enemies can access the network, copy any message, and inject arbitrary messages. Digital cryptography provides the basis for most computer security mechanisms.

The CIA Triad

- **Confidentiality:** protection against disclosure to unauthorised individuals.
- **Integrity:** protection against alteration or corruption of information.
- **Availability:** protection against interference with the means to access resources.

Threat Classes and Attack Methods

- **Leakage:** acquisition of information by unauthorised recipients.
- **Tampering:** unauthorised alteration of information.
- **Vandalism:** interference with system operation without direct gain to the perpetrator.
- **Eavesdropping:** obtaining copies of messages without authority.
- **Masquerading:** using another principal's identity without their authority.
- **Message tampering / Man-in-the-middle:** intercept, alter, and re-send messages.
- **Replaying:** storing intercepted messages and sending them later.
- **Denial of Service:** flooding a channel or resource to deny access to legitimate users.

Public-key certificate for Bob's Bank

1. *Certificate type*:	Public key
2. *Name*:	Bob's Bank
3. *Public key*:	K_{Bpub}
4. *Certifying authority*:	Fred – The Bankers Federation
5. *Signature*:	$\{Digest(field\ 2 + field\ 3)\}_{K_{Fpriv}}$

Figure 1.1 Threat model: the main categories of attack on a distributed system.

2. Cryptography

Cryptography is the science of using mathematics to encrypt and decrypt data. It enables storage and transmission of sensitive information on insecure networks. A **cryptographic algorithm** works with a **key** (a word, number, or phrase) to encrypt plaintext into ciphertext.

Security depends on: (1) the strength of the algorithm and (2) the secrecy of the key.

Alice's bank account certificate

1. *Certificate type*:	Account number
2. *Name*:	Alice
3. *Account*:	6262626
4. *Certifying authority*:	Bob's Bank
5. *Signature*:	$\{Digest(field\ 2 + field\ 3)\}_{K_{Bpriv}}$

Figure 2.1 Encryption and decryption: plaintext encrypted with key to produce ciphertext.

Two Main Classes

- **Shared secret keys (symmetric):** one key for both encryption and decryption; must be kept secret.
- **Public/private key pairs (asymmetric):** sender uses recipient's public key to encrypt; recipient uses private key to decrypt.

2.1 Secrecy and Integrity

Scenario – Shared secret key: Alice and Bob share key K_{AB}. Alice encrypts with $E(K_{AB}, M)$ and sends to Bob. Bob decrypts with $D(K_{AB}, M)$.

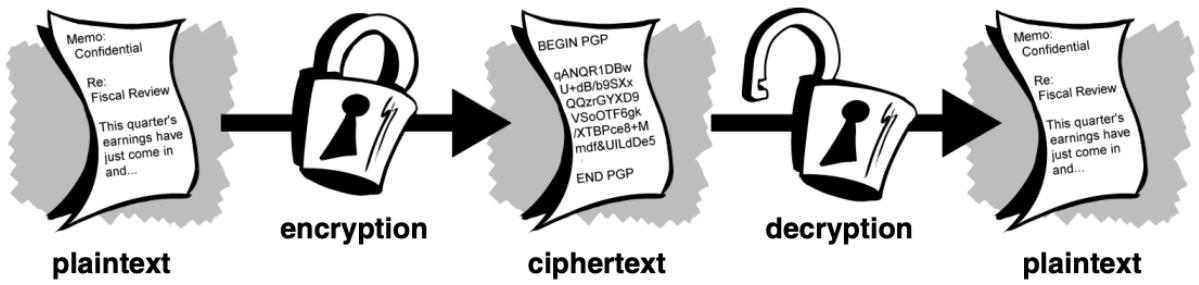

Figure 2.2 Secret communication: Alice encrypts with shared key K_AB; Bob decrypts with the same key.

2.2 Authentication

Scenario – Authenticated communication with a server: Sara is the authentication server holding keys K_A (for Alice) and K_B (for Bob).

- 1. Alice → Sara: unencrypted request for a ticket for Bob.
- 2. Sara → Alice: $\{\{Ticket\}K_B, K_{AB}\}K_A$ (ticket encrypted with K_B; session key encrypted with K_A).
- 3. Alice decrypts using K_A (from password; not transmitted; deleted after use). She obtains a valid ticket and session key K_{AB}.
- 4. Alice → Bob: $\{Ticket\}K_B$, identity, request R.
- 5. Bob decrypts ticket with K_B; obtains authenticated identity and K_{AB}.

Familiar names for the protagonists in security protocols

Alice	First participant
Bob	Second participant
Carol	Participant in three- and four-party protocols
Dave	Participant in four-party protocols
Eve	Eavesdropper
Mallory	Malicious attacker
Sara	A server

Figure 2.3 Authenticated communication with public keys: Alice obtains Bob's public key from a certificate, encrypts session key K_AB.

2.3 Digital Signatures

Verify to a third party that a message is an unaltered copy produced by the signer. Based on encrypting a digest (compressed form of the message) using the signer's private key.

- 1. Alice computes Digest(M).
- 2. Alice encrypts digest with her private key: appends $\{Digest(M)\}K_{Apriv}$ to M.
- 3. Bob decrypts $\{Digest(M)\}K_{Apriv}$ using Alice's public key K_{Apub} and compares with his computed Digest(M).
- 4. If they match: Alice is proven to be the originator and the document is proven unaltered.

Cryptography notations

K_A	Alice's secret key
K_B	Bob's secret key
K_{AB}	Secret key shared between Alice and Bob
K_{Apriv}	Alice's private key (known only to Alice)
K_{Apub}	Alice's public key (published by Alice for all to read)
$\{M\}_K$	Message M encrypted with key K
$[M]_K$	Message M signed with key K

Figure 2.4 Digital signature scenario: Alice signs with private key; Bob verifies with Alice's public key.

3. Digital Certificates

A certificate includes: (1) a public key, (2) certificate information (name, user ID), and (3) one or more digital signatures from a trusted authority. The signature vouches only that the identity information is bound to the public key.

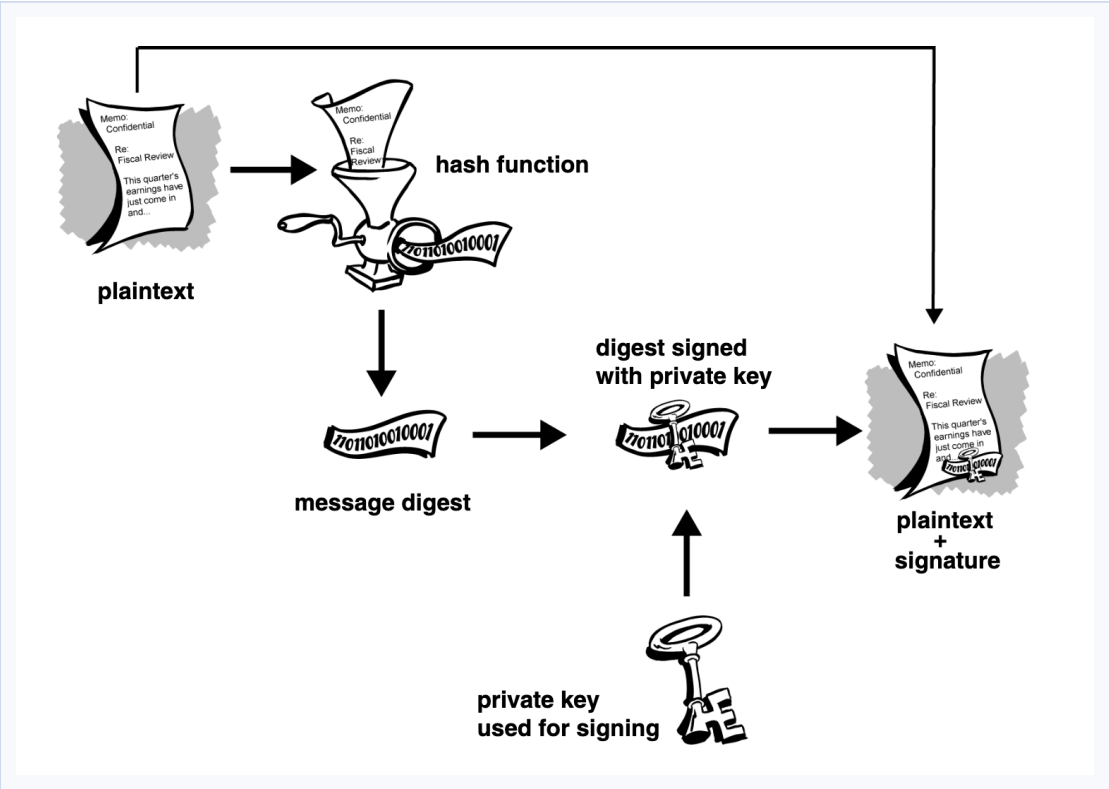

Figure 3.1 Digital certificate structure: public key, identity information, and digital signature from a CA.

4. Firewalls

Firewalls protect intranets by filtering incoming and outgoing communications. Messages are forwarded to the local recipient only for explicitly authorised communications. Limitations: not effective against attacks from inside; not effective against DoS attacks such as IP spoofing.

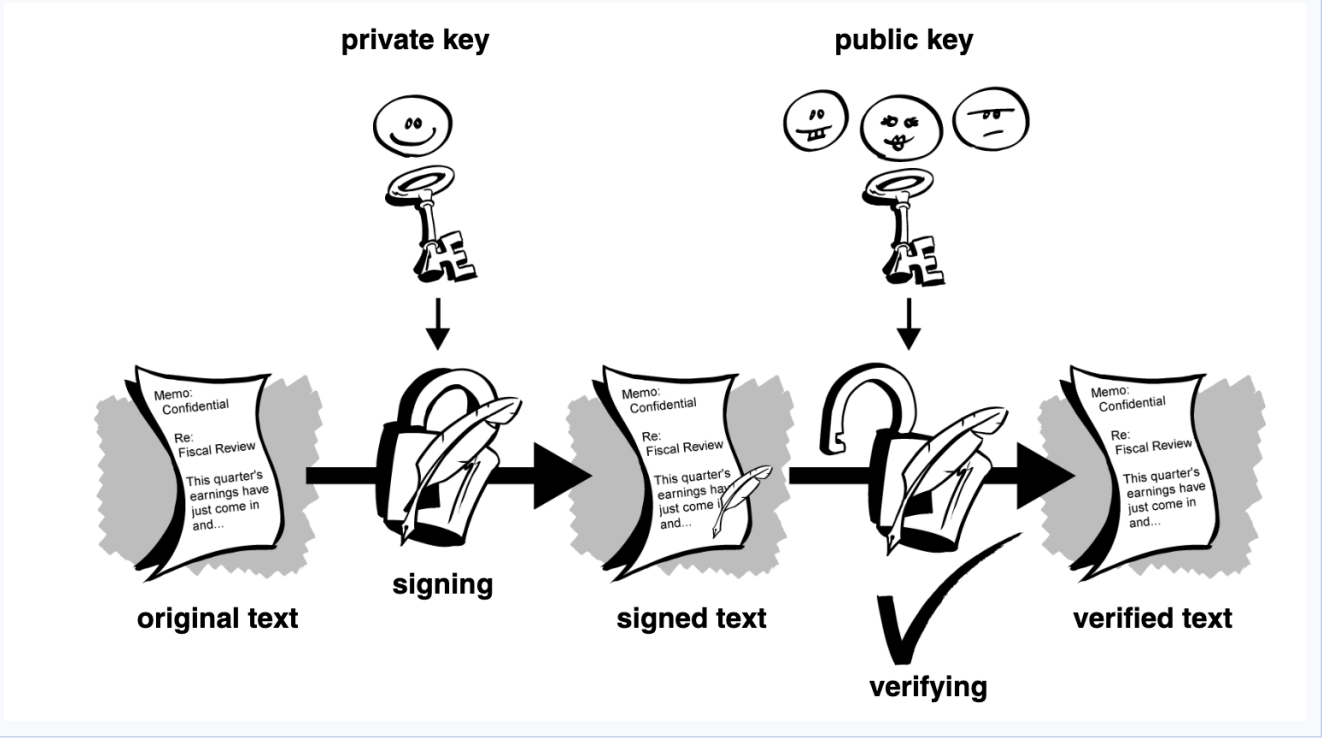

Figure 4.1 Firewall: gateway computer filters all inbound and outbound messages per the security policy.

5. Secure Digest Functions

A hash function ensures that if the information is changed in any way — even by a single bit — an entirely different output value is produced. This prevents taking a signature from one document and attaching it to another.

Exercises

- 1. Research Secret-Key (Symmetric) algorithms; write Medium article: ‘Secret Key Algorithms in Cryptography’.
- 2. Research Public-Key (Asymmetric) algorithms; write Medium article: ‘Public Key Algorithms in Cryptography’.
- 3. Research Digest Functions; explain MD5 and SHA-1; write Medium article: ‘Secure Digest Functions’.