Lecture 11 · SENG 41283 · Distributed and Cloud Computing

Cryptography

Conventional Cryptography · Caesar's Cipher · Public Key · PGP · Keys · Digital Signatures · Hash Functions · Certificates

1. Encryption and Decryption

- **Plaintext (cleartext):** data that can be read without special measures.
- **Encryption:** disguising plaintext so its substance is hidden; produces ciphertext.
- **Decryption:** reverting ciphertext to original plaintext.

2. What is Cryptography?

The science of using mathematics to encrypt and decrypt data, enabling storage or transmission of sensitive information on insecure networks. Cryptanalysis is the science of analysing and breaking secure communication.

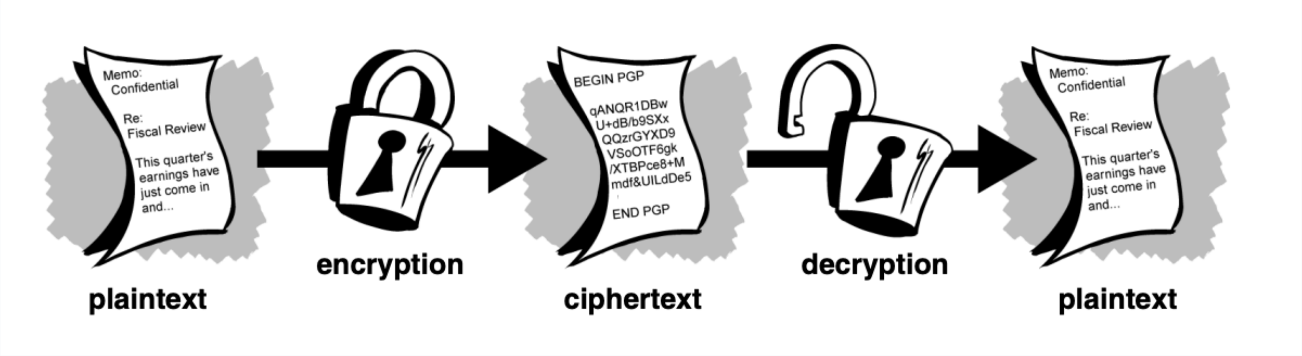

Figure 2.1 Encryption overview: plaintext + key + algorithm produces ciphertext; decryption reverses the process.

3. How Does Cryptography Work?

A **cryptographic algorithm** (cipher) works with a **key** (a word, number, or phrase) to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys. Security depends on: (1) strength of the algorithm; (2) secrecy of the key.

4. Conventional (Symmetric) Cryptography

One key used for both encryption and decryption. Benefits: very fast; excellent for data at rest. Drawback: the difficulty of secure key distribution is expensive.

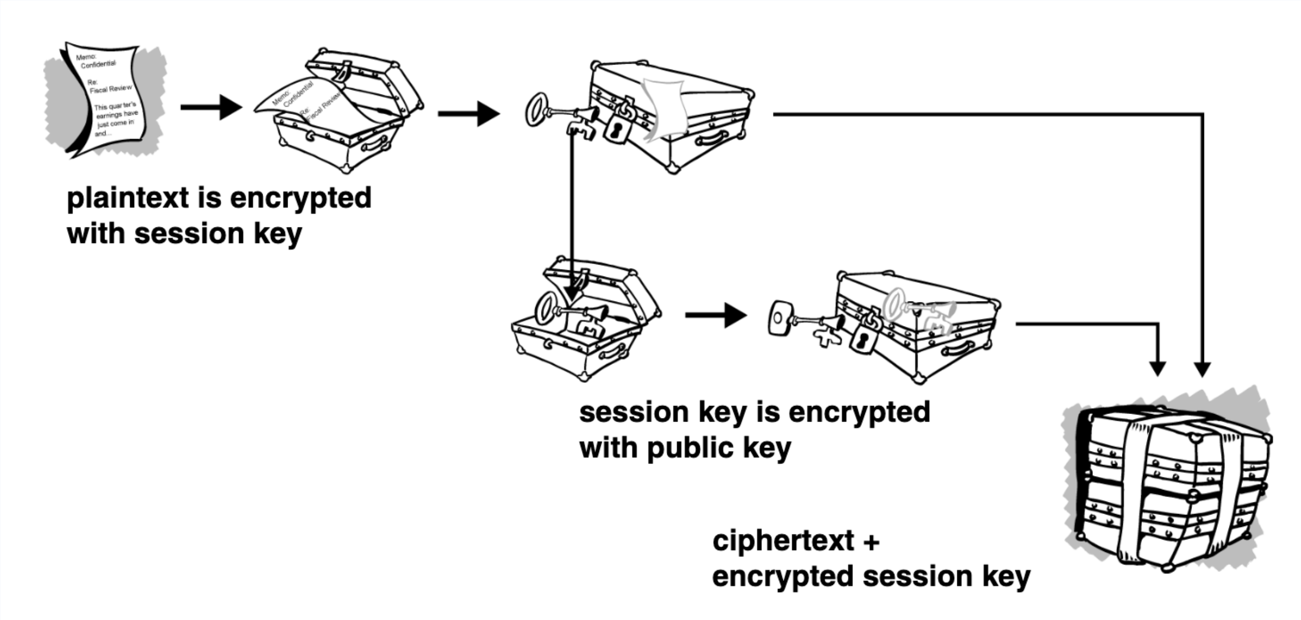
plaintext is encrypted with session key
session key is encrypted with public key
ciphertext + encrypted session key

Figure 4.1 Conventional cryptography: a single shared key is used for both encryption and decryption.

Caesar’s Cipher

A substitution cipher that offsets the alphabet. The algorithm is the offset; the key is the number of positions to offset.

```
Original: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Shift +3: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
S→V E→H C→F R→U E→H T→W
'SECRET' → 'VHFUHW'
```

5. Public Key Cryptography

Introduced by Diffie and Hellman (1975). An asymmetric scheme using a key pair: **public key** (encrypts; published to the world) and **private key** (decrypts; kept secret). Primary benefit: allows parties with no preexisting security arrangement to exchange messages securely.

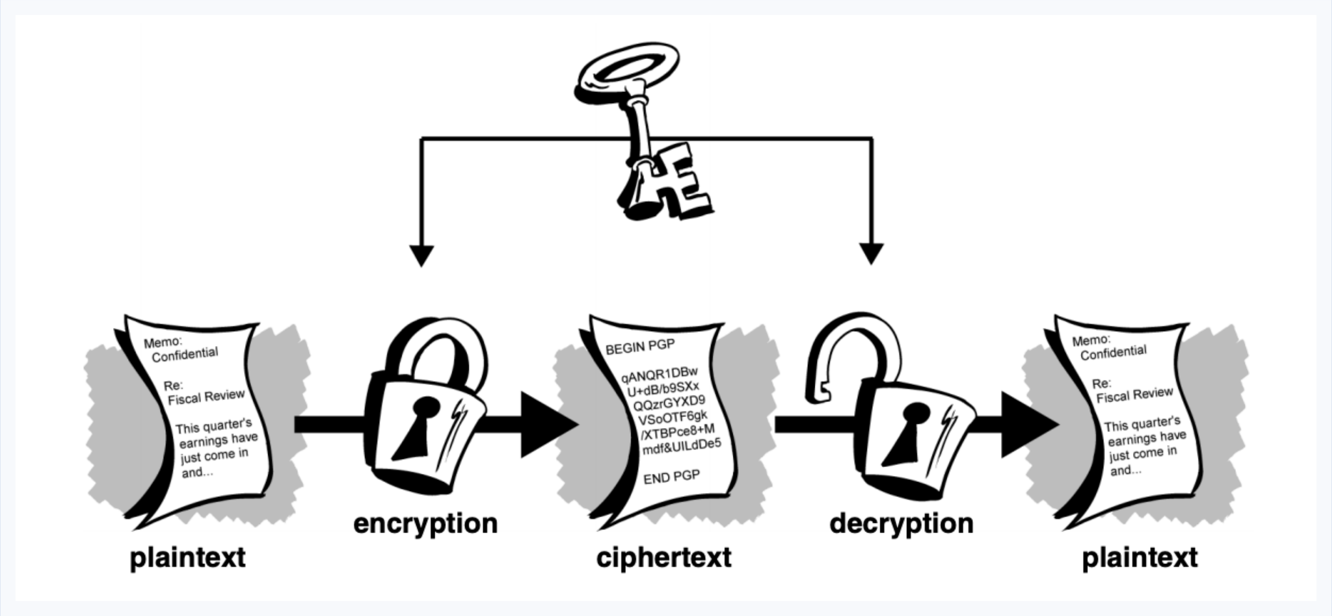
Memo: Confidential
Re: Fiscal Review
This quarter's earnings have just come in and...
plaintext
encryption
BEGIN PGP
qANQR1DBw U+dB/b9SXx QQzrGYXD9 VSoOTF6gk /XTBPce8+M mdf&UILdDe5
END PGP
ciphertext
decryption
Memo: Confidential
Re: Fiscal Review
This quarter's earnings have just come in and...
plaintext

Figure 5.1 Public key cryptography: sender uses recipient's public key to encrypt; recipient uses private key to decrypt.

- It is computationally infeasible to deduce the private key from the public key.
- **Examples:** ElGamal · RSA (Rivest, Shamir, Adleman) · Diffie–Hellman · DSA.

6. PGP — Pretty Good Privacy

A hybrid cryptosystem combining the best features of conventional and public key cryptography.

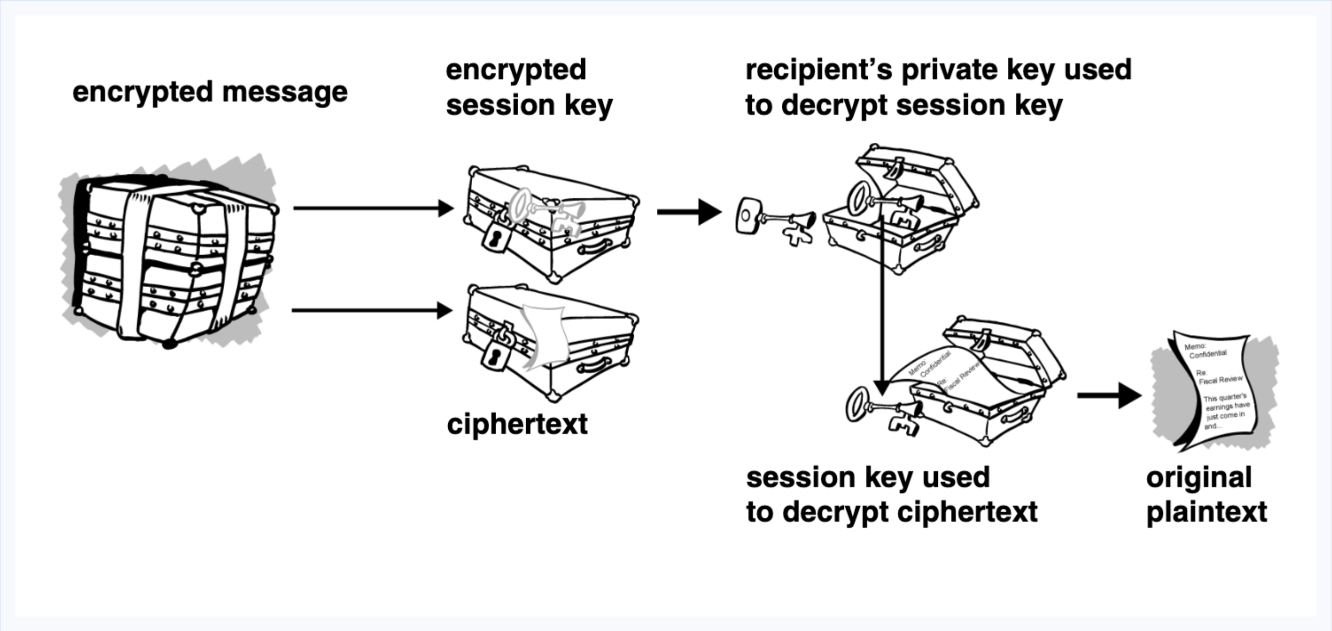
encrypted message
encrypted session key
recipient's private key used to decrypt session key
ciphertext
session key used to decrypt ciphertext
original plaintext

Figure 6.1 PGP encryption process: compress plaintext, create session key, encrypt with session key, encrypt session key with recipient's public key.

- 1. Compress plaintext (reduces patterns that cryptanalysis exploits).

- 2. Create a one-time session key from random mouse movements and keystrokes.
- 3. Encrypt plaintext with session key using a fast conventional algorithm.
- 4. Encrypt session key with recipient’s public key.
- 5. Transmit: encrypted session key + ciphertext.
- Decryption: recipient uses private key to recover session key; session key decrypts ciphertext.

7. Keys

Keys are very large numbers; key size is measured in bits. In public-key cryptography, a larger key means more secure ciphertext. The private key can always be derived from the public key given enough time and computing power, so keys must be large enough to be secure yet small enough to be applied quickly.

8. Digital Signatures

Verify the authenticity of information’s origin and that it was not altered in transit. Encrypt with your own **private key**; if information can be decrypted with your public key, it must have originated with you.

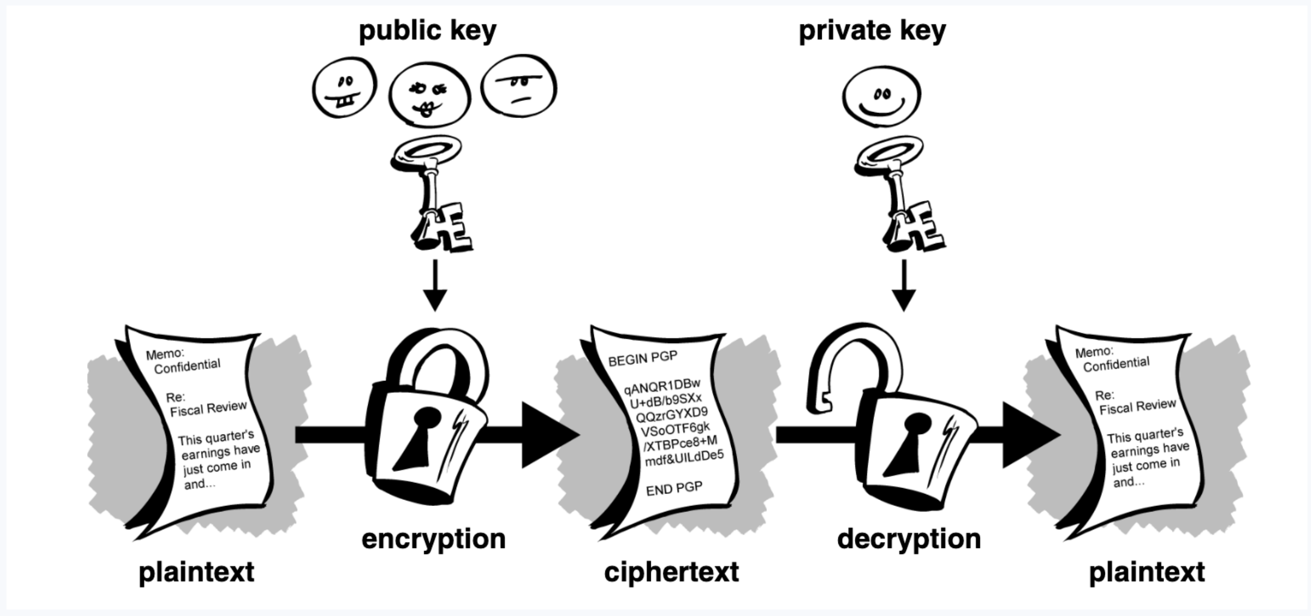

Figure 8.1 Digital signature: Alice encrypts the message digest with her private key; Bob verifies using Alice’s public key.

9. Hash Functions

If information is changed in any way — even by one bit — an entirely different output value is produced. It is impossible to attach a signature from one document to another, or to alter a signed message without breaking verification.

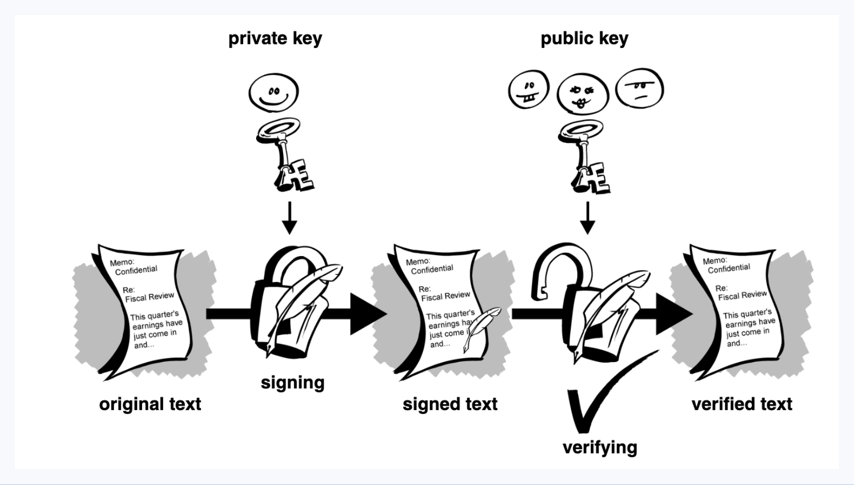
private key
public key
Memo: Confidential Re: Fiscal Review This quarter's earnings have just come in and...
signing
original text
signed text
verified text
verifying

Figure 9.1 Secure digest (hash) function: a small change in input produces a completely different output hash.

10. Digital Certificates

A certificate includes: (1) a public key, (2) identity information (name, user ID), and (3) one or more digital signatures. The signature vouches only that the identity information is bound to the public key, not the authenticity of the certificate as a whole.

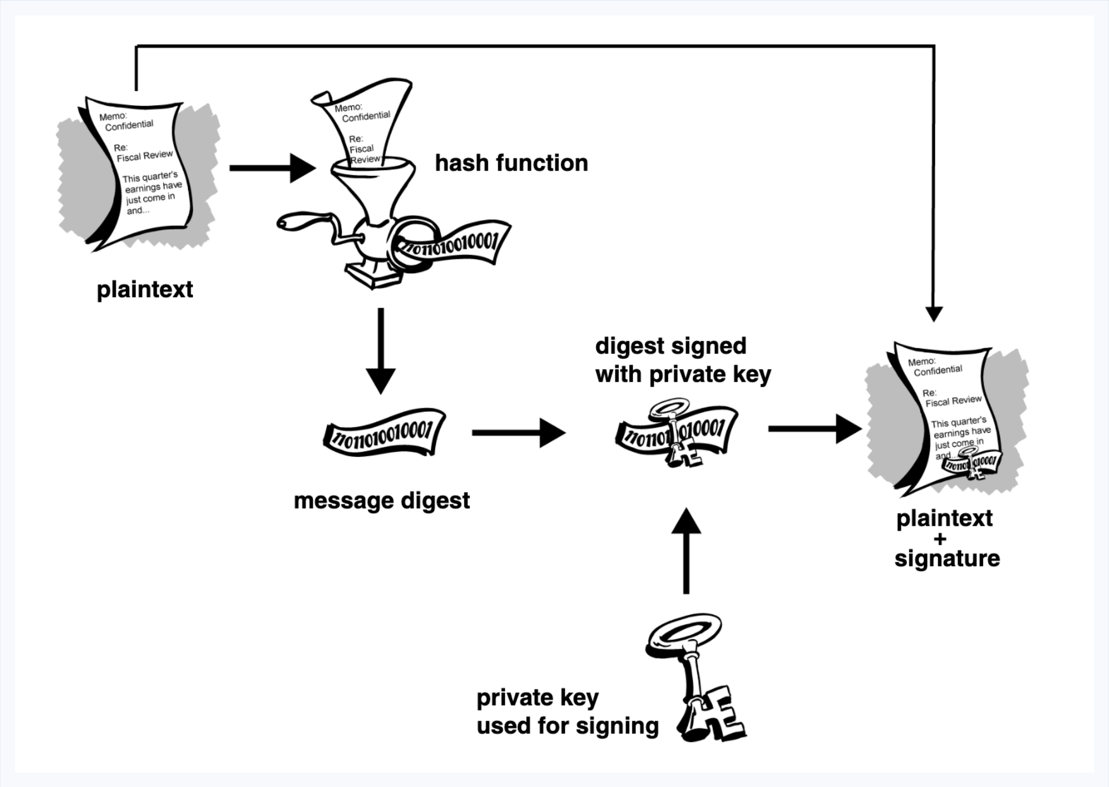

Figure 10.1 Digital certificate structure: public key, identity information, and digital signature from a certification authority.