6 Security, privacy and data integrity – Part 2

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	中文	Write it 3 times (English)		
plaintext	明文			
ciphertext	密文			
symmetric encryption	对称加密			
asymmetric encryption	非对称加密			
public key	公钥			
private key	私钥			
digital signature	数字签名			
denial of service	拒绝服务			
man-in-the-middle	中间人攻击			
checksum	校验和			

Recall

In **Part 1** you met threats (malware, phishing), protections (firewall, encryption, authentication), and data integrity (validation, verification, the check digit and parity). Part 2 looks at how encryption really works, two more network attacks, and stronger transfer checks.

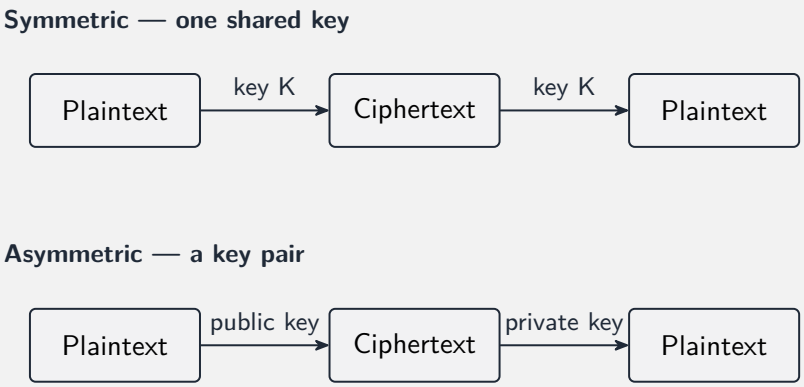
New ideas

Read these first. Each idea has a short worked example. Then do the Practice.

1 Symmetric vs asymmetric encryption

Encryption turns readable **plaintext** 明文 into scrambled **ciphertext** 密文 using a key.

- **symmetric encryption** 对称加密 uses **one shared key** to both lock and unlock —fast, but the key itself must be shared safely.
- **asymmetric encryption** 非对称加密 uses a pair: a **public key** 公钥 to lock (which anyone may have) and a **private key** 私钥 to unlock (kept secret). This solves the ”how do we share the key” problem.



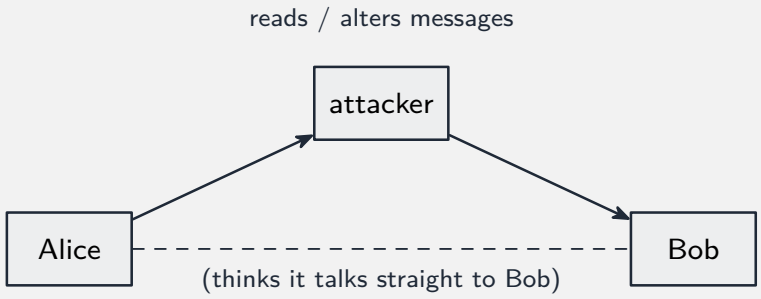
Worked example. To receive secret messages, Bob publishes his public key; anyone can lock a message with it, but only Bob’s private key can unlock it —so no secret key is ever shared.

2 Digital signatures and two more attacks

A **digital signature** 数字签名 proves *who* sent a message and that it was *not changed* on the way.

Two network attacks to know:

- a **denial of service** 拒绝服务 (DoS) attack floods a server with traffic so real users cannot get through;
- a **man-in-the-middle** 中间人攻击 attacker secretly sits between two parties, reading or altering their messages.



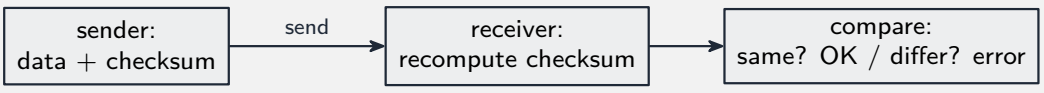
Worked example. On public Wi-Fi, a man-in-the-middle relays your messages to the bank while quietly reading them —both sides think they are talking directly.

Watch out: in asymmetric encryption you lock with the *recipient's public* key, not your own —only *their* private key can then unlock it.

■ 3 Checking a transfer arrived correctly

When data is sent, bits can flip. The receiver checks it:

- a parity bit catches a single flipped bit (Part 1);
- a **checksum** 校验和 is a summary number sent with the data; the receiver recomputes it and compares —a mismatch means an error. (A cyclic redundancy check, CRC, is a stronger version.)



Worked example. The sender adds the byte values to get a checksum of 204 and sends it too; the receiver re-adds the bytes —204 means the data is intact, anything else means an error.

Practice

6.1 In asymmetric encryption, state which key is used to **encrypt** a message sent to someone. [1]

6.2 State one difference between symmetric and asymmetric encryption. [2]

6.3 State what a digital signature proves about a message. [2]

6.4 Describe what a denial-of-service (DoS) attack does. [2]

6.5 Explain how a checksum lets the receiver detect an error in transferred data. [2]

6.6 Explain *why* asymmetric encryption solves a problem that symmetric encryption has. [2]

6.7 Challenge. A simple checksum just adds up the byte values. Explain why it might miss an error where two bytes are *swapped*. [2]