IGCSE COMPUTER SCIENCE • EXERCISE SHEET

2.3 Encryption

Name: _____ Class: _____ Date: _____ **Total: 8 marks**

KEY WORDS encryption 加密 • symmetric 对称 • symmetric encryption 对称加密 • asymmetric 非对称 • asymmetric encryption 非对称加密

Objective

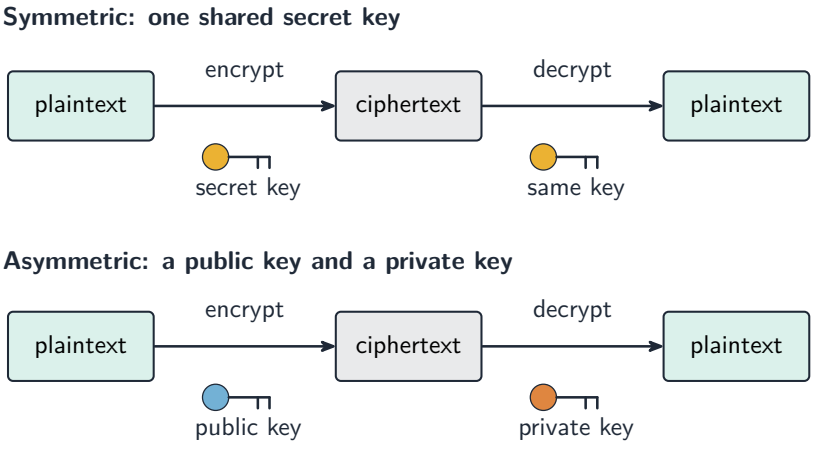
Build the skills to answer exam questions on **encryption** 加密 — why it is used, and **symmetric** 对称 and **asymmetric** 非对称 encryption.

You must be able to:

- explain the purpose of encryption (plaintext → ciphertext)
- describe symmetric encryption (one shared key)
- describe asymmetric encryption (public and private keys)

1 Worked examples

Symmetric vs asymmetric



Symmetric: one shared key. Asymmetric: a public key to encrypt, a private key to decrypt

- encryption scrambles data so it cannot be **understood** if intercepted (it does not stop interception).
- plaintext → (encrypt) → ciphertext.

2 Practice

2.1 State the purpose of encryption. [1]

2.2 Name the readable form of data before it is encrypted. [1]

3 Exam-style questions

3.1 In asymmetric encryption, data encrypted with a public key can be decrypted only with the: [1]

- **A** same public key
- **B** matching private key
- **C** shared secret key
- **D** checksum

3.2 A company chooses between symmetric and asymmetric encryption.

(a) State the main risk of symmetric encryption. [1]

(b) Explain why asymmetric encryption is more secure for sharing a key. [2]

3.3 State whether encryption stops data being intercepted, and explain. [2]

Solutions

2.1 to scramble data so it cannot be understood if intercepted.

2.2 plaintext.

3.1 B. It can be decrypted only with the matching private key.

3.2 (a) the shared secret key could be stolen while being sent.
(b) the public key encrypts and only the private key (kept secret) decrypts; so no secret key ever has to be shared.

3.3 no — encryption does not stop interception; it only stops the intercepted data from being understood.