IGCSE COMPUTER SCIENCE • EXERCISE SHEET

2.3 Encryption

Name: _____ Class: _____ Date: _____ **Total: 21 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

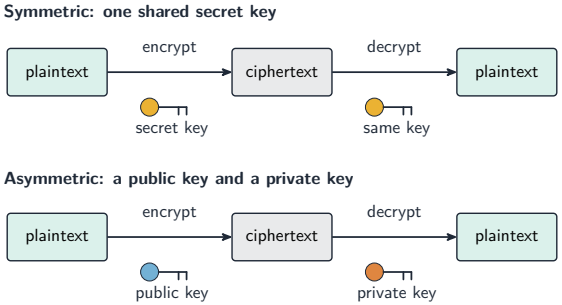
Build the skills to answer exam questions on **encryption** 加密 — why it is used, and **symmetric** 对称 and **asymmetric** 非对称 encryption.

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]

3.4 A company sends confidential files between two offices over the internet.

(a) Explain why encryption is needed, even though the data is already sent over a private connection. [2]

(b) Describe how **symmetric** encryption works, and state its main weakness. [4]

(c) Describe how **asymmetric** encryption works, naming both keys and explaining which one is used to encrypt and which to decrypt. [4]

(d) Explain the difference between *plaintext* and *ciphertext*, and state why encryption does not stop data being intercepted. [3]

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.

3.4 (a) Data travelling over the internet passes through equipment the company does not control and can be intercepted; encryption means an interceptor cannot understand the contents even if the data is captured.
(b) The **same key** is used to encrypt and to decrypt the data; the sender encrypts the plaintext with the key and the receiver applies the same key in reverse. Its weakness is **key distribution**: the key itself has to reach the receiver somehow, and if it is intercepted on the way the whole system is broken.
(c) Two mathematically related keys are used — a **public key** and a **private key**. The public key is published and anyone may use it to encrypt a message; only the matching **private key**, which is never shared, can decrypt it; so no secret has to be sent in advance.
(d) Plaintext is the original readable data; ciphertext is the scrambled version produced by the encryption algorithm. Encryption does not hide or block the transmission — the data can still be intercepted; it simply makes the intercepted data meaningless without the key.