

Exercise walk-through

Encryption ■ 2.3

eXercise

You must be able to

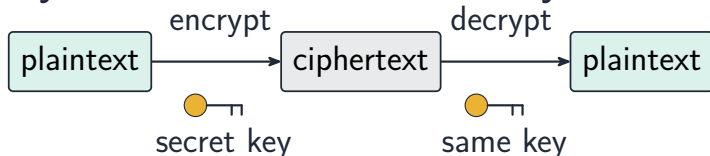
- explain the purpose of encryption (plaintext $\rightarrow$ ciphertext)
- describe symmetric encryption (one shared key)
- describe asymmetric encryption (public and private keys)

Method — Symmetric vs asymmetric

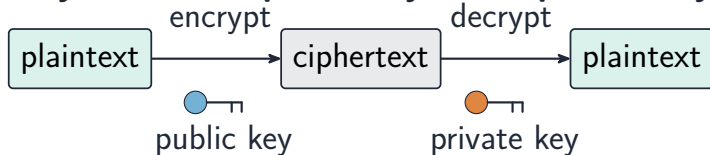
- encryption scrambles data so it cannot be **understood** if intercepted (it does not stop interception).
- plaintext $\rightarrow$ (encrypt) $\rightarrow$ ciphertext.

Method — Symmetric vs asymmetric

Symmetric: one shared secret key



Asymmetric: a public key and a private key



One shared key (symmetric) vs public/private keys (asymmetric)

Practice 2.1 ■ 1 mark

State the purpose of encryption.

Solution 2.1

Worked steps

to scramble data so it cannot be understood if intercepted **B1**.

Practice 2.2 ■ 1 mark

Name the readable form of data before it is encrypted.

Solution 2.2

Worked steps

plaintext **B1**.

Exam-style 3.1 ■ 1 mark

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

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

Solution 3.1

Method: Symmetric vs asymmetric

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



Worked steps

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

Exam-style 3.2 ■ 1 mark

A company chooses between symmetric and asymmetric encryption.

- (a) State the main risk of symmetric encryption.
- (b) Explain why asymmetric encryption is more secure for sharing a key.

Solution 3.2

Method: Symmetric vs asymmetric

Worked steps

- (a) the shared secret key could be stolen while being sent **B1**.
- (b) the public key encrypts and only the private key (kept secret) decrypts **M1**; so no secret key ever has to be shared **A1**.

Exam-style 3.3 ■ 2 marks

State whether encryption stops data being intercepted, and explain.

Solution 3.3

Method: Symmetric vs asymmetric

Worked steps

no — encryption does not stop interception **M1**; it only stops the intercepted data from being understood **A1**.