2.3 Encryption

Name: _____ Class: _____ Date: _____ **Total: 25 marks**

KEY WORDS encryption • symmetric • symmetric encryption • asymmetric • asymmetric encryption

Objective

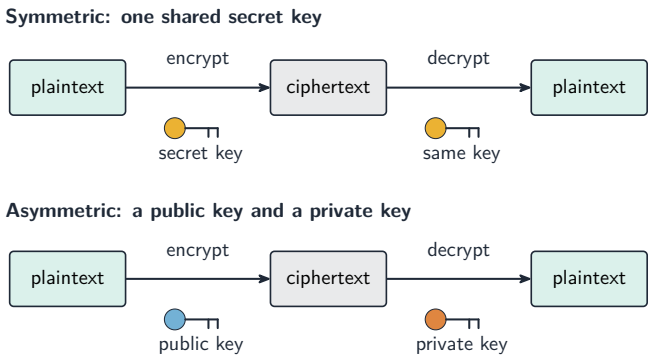
Build the skills to answer exam questions on **encryption** – why it is used, and **symmetric** and **asymmetric** encryption.

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 Key knowledge and worked examples

■ Symmetric vs asymmetric

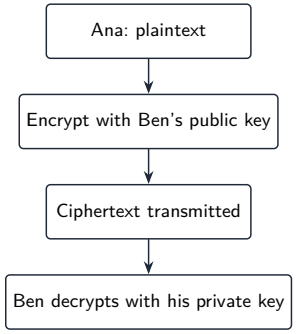


Symmetric: one shared key. Asymmetric: a public key to encrypt, a private key to decrypt

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

■ Worked application: Choose the key without sharing the secret

In a fictional message exchange, Ben publishes his public key but keeps his private key secret. Ana encrypts a message intended for Ben using Ben's public key. Ben decrypts it with his private key. Publishing Ana's private key or encrypting with an unrelated recipient's public key does not meet this purpose. Encryption protects the understandable content if transmission is intercepted; it does not stop an attacker copying the encrypted data, and it does not by itself prove who originally sent a message. For symmetric encryption, sender and receiver use the same secret key and must arrange to share it securely.



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]

3.5 Ana sends an encrypted message intended only for Ben using asymmetric encryption. Name the key she uses and the key Ben uses. Explain why encrypting the message does not prevent interception. [4]

Solutions

Each answer shows the steps, then the **result**.

2.1

- encryption changes readable data into a scrambled form
- purpose: so it **cannot be understood if intercepted**

2.2

- readable data before encryption is called **plaintext**

3.1 B

- data encrypted with a public key is decrypted only with the **matching private key**
- A is the same public key; C is symmetric; D is error-checking, not decryption

3.2

(a)

- both sides share one secret key
- main risk: the **shared key could be stolen while being sent**

(b)

- the public key encrypts; only the private key (kept secret) decrypts
- **no secret key ever has to be shared**

3.3

- encryption does **not** stop interception
- it only stops the intercepted data from being **understood**

3.4

(a)

- data on the internet passes through equipment the company does not control and can be intercepted
- encryption means an interceptor **cannot understand** the contents even if they capture them

(b)

- the **same key** encrypts and decrypts
- sender encrypts plaintext with the key; receiver applies the same key in reverse
- weakness is **key distribution**: if the key is intercepted on the way, the whole system is broken

(c)

- two related keys: a **public key** and a **private key**
- anyone may use the published public key to **encrypt**
- only the matching **private key**, never shared, can **decrypt**
- so no secret has to be sent in advance

(d)

- **plaintext** is the original readable data
- **ciphertext** is the scrambled version
- encryption does not block the transmission – it only makes intercepted data **meaningless without the key**

3.5

Ana uses Ben's public key; Ben uses his private key; an attacker can still copy or capture the transmitted ciphertext, but cannot readily understand its content without the needed decryption key.