

Exercise walk-through

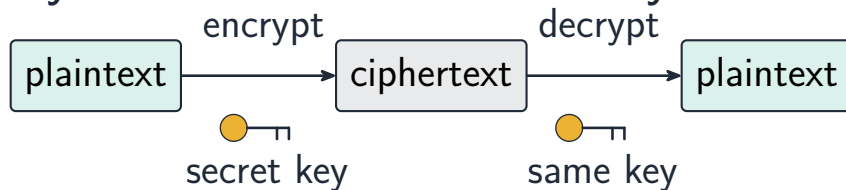
2.3

Encryption

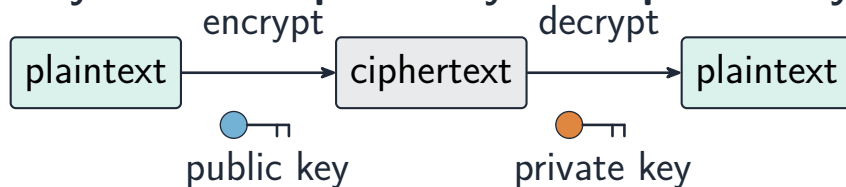
IGCSE Computer Science

Encryption

Symmetric: one shared secret key



Asymmetric: a public key and a private key



- **symmetric** : one **shared** key encrypts and decrypts
- **asymmetric** : a **public key** encrypts, a **private key** decrypts

Encryption does **not** stop interception – it stops the data being **understood**. Asymmetric never shares a secret key.

Plaintext, ciphertext, and what encryption really promises

Plaintext

Plaintext is the readable data before encryption – what a thief wants.

Ciphertext

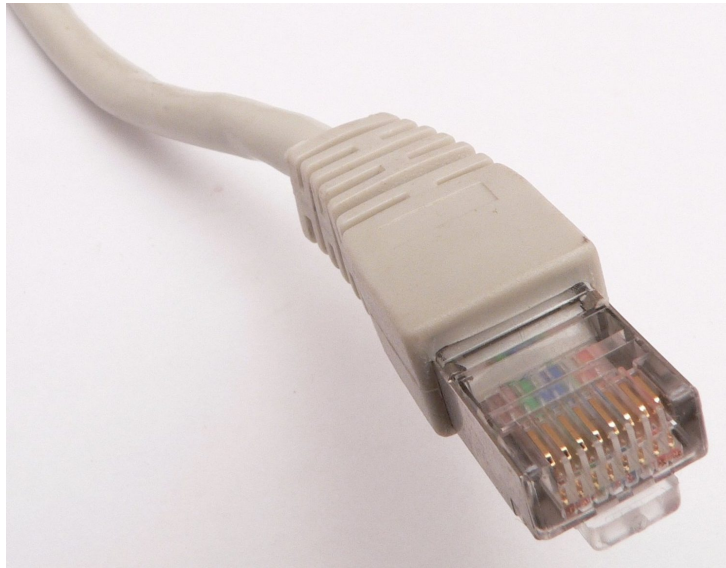
After encryption it becomes **ciphertext** : still readable as characters, but meaningless without the key.

Intercepted

Encryption does **not** stop data being **intercepted** ; it stops the intercepted data being *understood*.

State the promise precisely in an exam: confidentiality, not delivery. The packet can still be caught – it just cannot be read.

An Ethernet cable with an RJ45 plug



An Ethernet cable with an RJ45 plug, often used to carry data on a wired network

Exam tips

- Data is sent in **packets** (a header with the addresses and packet number, a payload, and a trailer). Packets can take different routes and arrive out of order, then are reordered by their packet numbers.
- Match the transmission types: **serial** (one bit at a time, good over long distances) vs **parallel** (several bits at once, short distances); **simplex** / **half-duplex** / **full-duplex** describe the direction.
- A single **parity bit** only shows *that* an error happened; a **parity block** locates the exact wrong bit – the row and the column that both fail.
- Learn the error-detection methods and what each does: parity check, checksum, echo check, ARQ, and the check digit (for typed-in numbers).
- **Symmetric** encryption uses one shared key; **asymmetric** uses a public key to encrypt and a private key to decrypt, so no secret key is ever shared.

Exercises 2.1-2.2

2.1 State the purpose of encryption.

[1]

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

[1]

Exercises 2.1·2.2

2.1 State the purpose of encryption.

[1]

2.1

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

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

[1]

2.2

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

Exercise 3.1

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

Exercise 3.1

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

3.1 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

Exercise 3.2 (a)

3.2 A company chooses between symmetric and asymmetric encryption.

(a) State the main risk of symmetric encryption.

[1]

Exercise 3.2 (a)

3.2 A company chooses between symmetric and asymmetric encryption.

(a) State the main risk of symmetric encryption.

[1]

(a)

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

Exercise 3.2 (b)

3.2 A company chooses between symmetric and asymmetric encryption.

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

[2]

Exercise 3.2 (b)

3.2 A company chooses between symmetric and asymmetric encryption.

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

[2]

(b)

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

Exercise 3.3

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

[2]

Exercise 3.3

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

[2]

3.3

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

Exercise 3.4 (a)

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]

Exercise 3.4 (a)

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]

(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

Exercise 3.4 (b)

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

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

[4]

Exercise 3.4 (b)

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

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

(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

Exercise 3.4 (c)

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

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

Exercise 3.4 (c)

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

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

(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

Exercise 3.4 (d)

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

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

Exercise 3.4 (d)

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

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

(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**

Exercise 3.5

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]

Exercise 3.5

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]

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.