IGCSE COMPUTER SCIENCE • EXERCISE SHEET

5.3 Cyber security

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

Objective

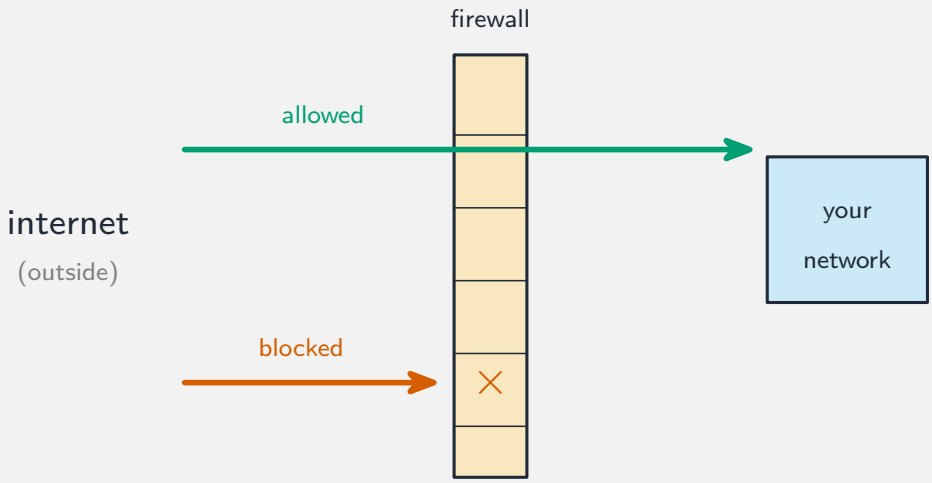
Build the skills to answer exam questions on **cyber security** 网络安全—the threats, types of **malware** 恶意软件, and methods to keep data safe.

You must be able to:

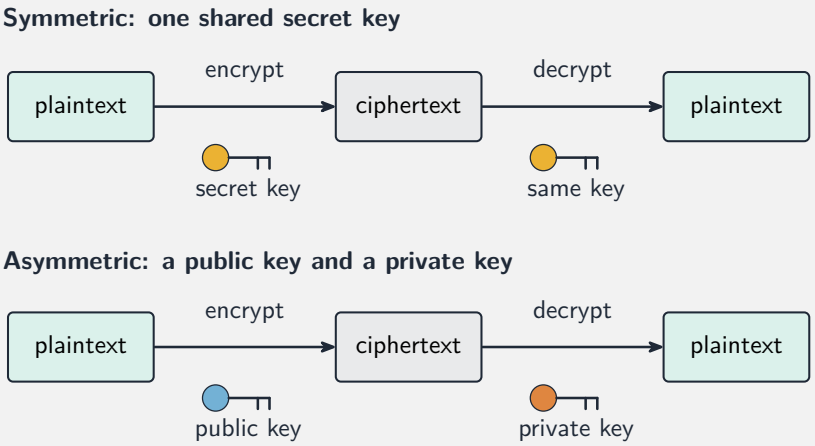
- describe threats (brute force, DDoS, phishing, pharming, social engineering)
- describe the types of malware
- describe security methods (firewall, authentication, anti-malware)

1 Worked examples

Threats and protection



A firewall checks data in/out of a network and blocks anything not allowed



Encryption is a key security measure against interception

- **threats:** brute force, data interception, DDoS, hacking, malware, pharming, phishing, social engineering.
- **malware:** virus, worm, Trojan, spyware, adware, ransomware.

2 Practice

2.1 State what a brute force attack is. [1]

2.2 State what ransomware does. [1]

3 Exam-style questions

3.1 A firewall protects a network by: [1]

- **A** scanning for viruses
- **B** checking data in/out and blocking what is not allowed
- **C** encrypting files
- **D** hiding the IP address

3.2 A company wants to protect its data.

(a) Describe what a phishing attack is. [2]

(b) State two methods (other than a firewall) to keep data safe. [2]

3.3 State the difference between a virus and a worm. [2]

4 Go further

You are now ready for the real exam questions on this subtopic. Open the **5.3 Cyber security** past-paper sheet in the Library, or try these in **Practice mode**:

- 0478/11 N25 —Q4 (cyber security threats)
- 0478/13 N25 —Q4 (protection methods)

Solutions

2.1 trying many passwords very quickly until the right one is found.

2.2 it locks your files and demands payment to unlock them.

3.1 B. A firewall checks data in/out and blocks anything not allowed.

3.2 (a) fake emails/messages that trick you into giving away private details.
(b) any two of: authentication (password/biometrics/two-step); anti-malware; access levels; automatic updates; proxy server.

3.3 a virus attaches to a file and copies itself when the file is opened; a worm copies itself across a network on its own, without a file being opened.