IGCSE COMPUTER SCIENCE • EXERCISE SHEET

5.3 Cyber security

Name: _____ Class: _____ Date: _____ **Total: 28 marks**

KEY WORDS cyber security 网络安全 • malware 恶意软件 • firewall 防火墙 • phishing 网络钓鱼 • proxy server 代理服务器

Objective

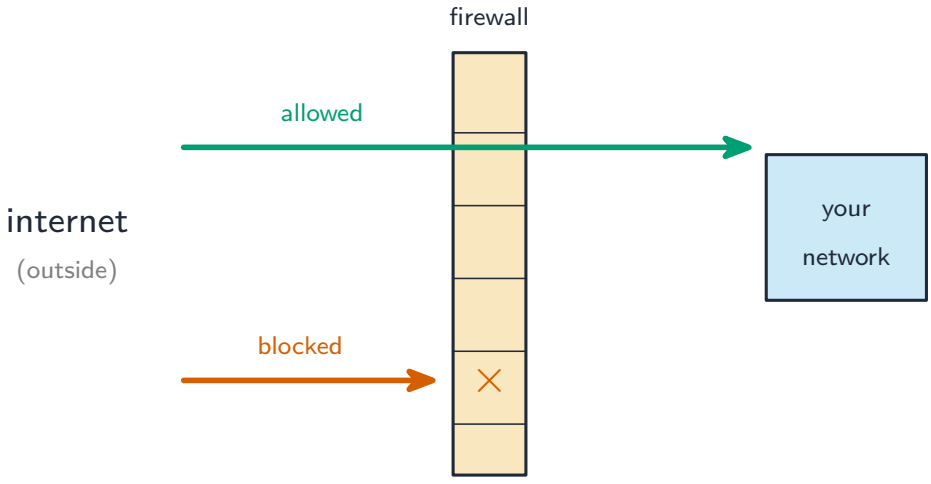
Build the skills to answer exam questions on **cyber security** 网络安全 — the threats, types of **malware** 恶意软件, and methods to keep data safe.

You must be able to:

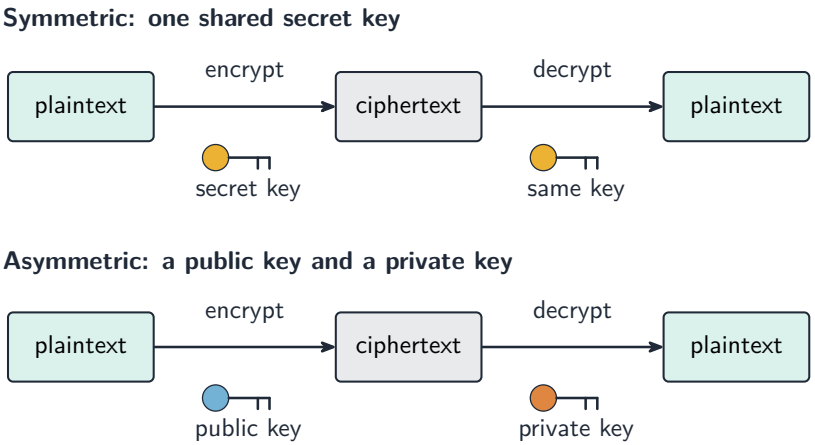
- describe threats (brute force, DDoS, phishing, pharming, social engineering)
- describe the types of malware
- describe security methods (firewall, authentication, anti-malware)

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.

■ Keeping data safe: which measure answers which risk

Encryption 加密 scrambles data with a key so that an interceptor gets **ciphertext** 密文 they cannot read; the plaintext is recovered with the key. It does not stop the data being taken, it makes what is taken useless. **Symmetric encryption** uses the same key to encrypt and decrypt, so the key itself must be exchanged safely; **asymmetric encryption** uses a public key to encrypt and a matching private key to decrypt, so nothing secret has to be sent.

Secure sockets layer (SSL) and its successor TLS encrypt the traffic between a browser and a web server. The browser checks the site's **digital certificate**, then the two agree a session key. You can tell it is in use because the address begins `https` and a padlock appears.

Firewall 防火墙: examines traffic entering and leaving the network, compares it with a set of criteria, blocks what fails, logs traffic, and can block named sites or addresses.

Proxy server 代理服务器: sits between the user and the internet, so the web server never sees the user's own address. It can filter traffic, keep a cache of pages so they load faster, and act as a firewall.

Access rights 访问权限: each user gets only the permissions their role needs (read, read-and-write, none), so a person who is not authorised cannot see or change a file even after logging in.

Authentication 身份验证: passwords, biometrics (fingerprint, face, iris), and two-step verification, which sends a one-time code to a device the real user holds.

Worked example. A hospital keeps patient records on a server used by doctors and receptionists. Suggest measures. Encrypt the records so a stolen copy is unreadable; use access rights so receptionists see only appointment details while doctors see the

> medical notes; use biometrics or two-step verification, so a stolen password alone is not enough; put a firewall between the server and the internet to block unauthorised traffic.

2 Practice

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

2.2 State what ransomware does. [1]

2.3 Give the name of the data before and after encryption. [2]

2.4 Identify two tasks performed by a proxy server. [2]

2.5 Explain why encryption does not stop data being intercepted. [2]

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]

3.3 An online bank protects its customers' data.

(a) Explain what happens to data when it is encrypted, using the terms plaintext and ciphertext. [2]

(b) Identify the protocol that encrypts the connection between a customer's browser and the bank's server, and give one way the customer can tell it is being used. [2]

(c) Describe two tasks a firewall performs for the bank's network. [2]

(d) Bank staff have different access rights. Explain how access rights protect customer data even from someone who has logged in successfully. [2]

(e) The bank adds two-step verification. Describe how it works and explain why it is safer than a password alone. [3]

(f) Explain one advantage of asymmetric encryption over symmetric encryption when a customer first connects. [2]

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.

2.3 Plaintext before, ciphertext after.

2.4 Any two of: it filters traffic; it keeps a cache of web pages so they load faster; it hides the user's IP address from the web server; it acts as a firewall.

2.5 Encryption only scrambles the data; an interceptor can still take a copy, but without the key the ciphertext is meaningless to them.

3.3 (a) The readable plaintext is scrambled using a key so that it becomes ciphertext, which cannot be understood without the matching key to decrypt it.
(b) SSL, or its successor TLS; the address begins with `https` or a padlock is shown in the address bar.
(c) Any two of: it examines the traffic entering and leaving the network; it compares that traffic with a set of criteria and blocks anything that fails; it keeps a log; it blocks named sites or IP addresses.
(d) Each user is given only the permissions their job needs, so a receptionist who logs in cannot open or change files reserved for doctors.
(e) After the password is accepted, a one-time code is sent to a device the real user holds, such as their phone; the user must enter that code to complete the log-in; a thief who has only the password still cannot get in without the device.
(f) With asymmetric encryption the bank publishes a public key that anyone may use to encrypt, so no secret key has to be sent over the internet where it could be intercepted, unlike symmetric encryption.