2.3 Network security

Name: _____ Class: _____ Date: _____ **Total: 19 marks**

KEY WORDS authentication • authorization • symmetric encryption • asymmetric encryption • digital certificate

Objective

Build the skills to answer exam questions on **network security** – threats, firewalls, authentication and encryption.

You must be able to:

- describe common threats: malware, phishing, interception, unauthorised access, denial of service
- explain how a firewall, **authentication** and multi-factor authentication protect a network
- tell authentication from **authorization**
- compare **symmetric encryption** with **asymmetric encryption**, and explain a **digital certificate**

1 Key knowledge and worked examples

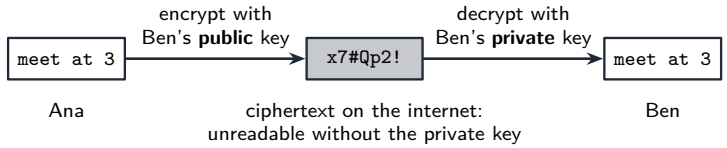
Study these first. Each one shows the method for a question type used later.

■ Key knowledge: threats and countermeasures

Threat	Countermeasure
malware, ransomware	anti-malware, updates, backups
phishing	user training, spam filters, MFA
interception	encryption (HTTPS, VPN)
weak passwords	password rules, MFA
denial of service	firewall rules, extra servers

- Authentication: **who** you are (password, phone, fingerprint). Authorization: **what** you may do.
- Multi-factor authentication (MFA) needs two kinds: e.g. a password **and** a code on a phone.

■ Worked example: public-key encryption



Ana sends Ben a secret message over the internet.

1. Ben publishes his **public** key; anyone may have it.
2. Ana encrypts with Ben's public key.
3. Only Ben's **private** key, which never leaves him, can decrypt it.
4. An eavesdropper sees only ciphertext.

	Symmetric	Asymmetric
keys	one shared key	public and private pair
speed	fast	slower
key sharing	must be done safely	public key shared openly

HTTPS uses asymmetric encryption to agree a session key, then symmetric encryption for speed. The site's digital certificate, signed by a trusted authority, proves the public key is really the site's.

2 Practice

2.1 Distinguish authentication from authorization, with a school example. [2]

2.2 Explain how a firewall protects a school network. [2]

2.3 Explain why multi-factor authentication is more secure than a password alone. [2]

3 Exam-style questions

3.1 Which key decrypts a message encrypted with Ben's public key? [1]

- **A** Ana's public key
- **B** Ana's private key
- **C** Ben's public key
- **D** Ben's private key

3.2 What does a website's digital certificate show? [1]

- **A** that the site has no malware
- **B** that the public key belongs to that website
- **C** the user's password
- **D** the site's IP address

3.3 Which countermeasure best limits the damage of ransomware? [1]

- **A** a faster network
- **B** regular backups kept offline
- **C** a longer domain name
- **D** UDP instead of TCP

3.4 A clinic stores patient records on a server that staff reach from the clinic and from home.

(a) Identify **two** threats to the records, and for each describe a suitable countermeasure. [4]

(b) Explain why the records sent to staff at home are encrypted. [2]

(c) The clinic uses symmetric encryption for the records. Explain the problem of sharing the key, and how asymmetric encryption solves it. [3]

(d) A receptionist can read appointment times but not medical notes. Identify the security measure that does this. [1]