Exercise walk-through

2.3
Network security

International Baccalaureate · IB Diploma · Computer Science · SL

Networks · 2.1

Reasoning

Packets carry addressed data through a network. A layered model separates responsibilities such as application meaning, transport delivery and network routing. Bandwidth describes capacity; throughput is the achieved data rate; latency is delay. throughput: Achieved rate of useful data transfer. latency: Delay experienced in communication.

Networks · executable trace

- Trace the state changes and boundary guard.
- Run the boundary case and compare the printed output.

```
size_Mb, rate_Mbps, propagation_s = 12, 3, 0.10
for rate in [rate_Mbps, 2 * rate_Mbps]:
    transmission_s = size_Mb / rate
    print(round(transmission_s + propagation_s, 2))
```

Exercises 2.1–2.3

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]

Exercises 2.1·2.3

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

2.1

- authentication checks who the user is: e.g. a student logs in with a password
- authorization decides what they may do: e.g. a student can read but not change grades

---

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

2.2

- it checks each packet against rules, such as allowed addresses, ports and protocols
- it blocks traffic that breaks the rules, keeping out unwanted or harmful connections

---

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

2.3

- a second factor, such as a code on the user's phone, is also needed
- a stolen or guessed password alone is then not enough to log in

Exercises 3.1·3.2

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

Exercises 3.1·3.2

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

3.1 D

- only the matching private key decrypts

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

3.2 B

- signed by a trusted authority

Exercise 3.3

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

Exercise 3.3

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

3.3 B

- the data can be restored without paying

Exercise 3.4 (a)

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]

Exercise 3.4 (a)

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]

(a) Any two threats, each with a matching countermeasure, e.g.:

- phishing for staff passwords; MFA and staff training
- interception of records sent to home; encryption over a VPN or HTTPS
- malware or ransomware; anti-malware, updates and offline backups

Exercise 3.4 (b)

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

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

Exercise 3.4 (b)

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

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

(b)

- the data travels over the public internet, where it can be intercepted
- encrypted records cannot be read without the key, protecting patient privacy

Exercise 3.4 (c)

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

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

Exercise 3.4 (c)

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

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

(c)

- the same key encrypts and decrypts, so it must reach every staff member without being intercepted
- with asymmetric encryption, each person publishes a public key for encrypting
- only their private key, never sent, can decrypt; often used to send the symmetric key safely

Exercise 3.4 (d)

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

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

Exercise 3.4 (d)

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

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

(d)

- **authorization**: access rights or permissions per user role