Solutions

Marking: **M1** a correct method, **A1** the correct answer, **B1** an independent mark.

Each answer shows the steps, then the **result**.

2.1

encryption: confidentiality

MAC: integrity, from someone who shares the key

signature: integrity and proof of origin that anyone can check (non-repudiation)

2.2

symmetric: $100 \times 99/2 = \mathbf{4950}$

public key: **100** key pairs

2.3

an attacker in the middle could send their own public key

the certificate is a CA's signature binding the key to the bank's name, which the attacker cannot forge

2.4

56-bit: $2^{56} \approx 7.2 \times 10^{16}$ keys

7.2×10^4 s $\approx$ **20 hours**

128-bit: 3.4×10^{26} s, about 10^{19} years

3.1

(a) allow, rule 1; allow, rule 2; deny, rule 3; deny, rule 4

(b) anything not allowed on purpose is blocked, so a forgotten service is not exposed

(c) it remembers connections, so replies to connections started from inside are let in without opening rules for all incoming traffic

3.2

(a) $10^6 \times 30 = 3 \times 10^7$ entries; $\times 256$ B $\approx$ **7.7 GB**

(b) the server stores nothing for a SYN; it puts a keyed hash of the connection details in its sequence number and rebuilds the state only when a real ACK returns it

(c) the attacker sends small requests with the victim's forged address to servers that send much larger replies to the victim

3.3

(a) read the password and the session cookie; change pages in transit, e.g. add a fake login form

(b) the data is encrypted and checked for changes, and the certificate proves the browser is talking to the real portal's name

exercises.lol exercises.com.cn

(c) TLS only proves the site owns the name in the address bar, and the attacker owns that name; a second factor such as a code or a security key, or a password manager that fills only on the real domain

(d) HTTPS everywhere with HSTS so the browser never uses HTTP, plus a second factor for staff and students: TLS stops eavesdropping, and the second factor makes a stolen or phished password not enough