Exercise walk-through

Asymmetric Cryptography ▪ 5.4

eXercise

You must be able to

- explain the roles of a **public key** 公钥 and a **private key** 私钥
- say which key encrypts and which decrypts when sending a secret
- state that asymmetric encryption solves the key-sharing problem

Method — The key pair

A key pair has a public key (shared with everyone) and a private key (kept secret). They are mathematical inverses: what one locks, only the other unlocks.

Method — Sending a secret

To send Bob a secret, encrypt with Bob's public key. Only Bob's private key can decrypt it - so no shared secret ever had to be exchanged in advance.

Practice 2.1 ▪ 1 mark

State which key you use to encrypt a message you are sending to someone.

Solution 2.1

Method: Sending a secret

Worked steps

the recipient's public key B1.

Practice 2.2 ▪ 2 marks

Explain why the private key must be kept secret.

Solution 2.2

Method: The key pair

Worked steps

the private key is the only key that can decrypt messages sent to its owner B1; if it leaks, an adversary can read those messages B1.

Practice 2.3 ▪ 1 mark

State the main advantage of asymmetric over symmetric encryption.

Solution 2.3

Worked steps

it solves the key-sharing problem - no shared secret must be exchanged first B1.

Exam-style 3.1 ▪ 1 mark

To send Bob an encrypted message, you use

A Bob's public key

B Bob's private key

C your private key

D no key

Solution 3.1

A Bob's public key ✓

B Bob's private key

C your private key

D no key

Worked steps

A. encrypt with the recipient's public key.

Exam-style 3.2 ▪ 1 mark

Which is an asymmetric encryption algorithm?

A AES

B RSA

C WPA3

D SHA-256

Solution 3.2

A AES

B RSA ✓

C WPA3

D SHA-256

Worked steps

B. RSA is asymmetric; AES is symmetric.

Exam-style 3.3 ▪ 1 mark

Alice wants to send Bob a confidential file over the internet.
(a) State which key Alice uses to encrypt it.
(b) Explain why only Bob can read the file.

Solution 3.3

Method: Sending a secret

Worked steps

(a) Bob's public key B1. (b) only Bob's matching private key can decrypt it B1, and Bob keeps that private key secret B1.