AP CYBERSECURITY • EXERCISE SHEET

5.4 Asymmetric Cryptography

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

Objective

Build the skills to answer exam questions on **asymmetric encryption** 非对称加密 and public/private key pairs.

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

1 Worked examples

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

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.

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.

2 Practice

2.1 State which key you use to encrypt a message you are sending to someone. [1]

2.2 Explain why the private key must be kept secret. [2]

2.3 State the main advantage of asymmetric over symmetric encryption. [1]

3 Exam-style questions

3.1 To send Bob an encrypted message, you use [1]

- **A** Bob's public key
- **B** Bob's private key
- **C** your private key
- **D** no key

3.2 Which is an asymmetric encryption algorithm? [1]

- **A** AES
- **B** RSA
- **C** WPA3
- **D** SHA-256

3.3 Alice wants to send Bob a confidential file over the internet.

(a) State which key Alice uses to encrypt it. [1]

(b) Explain why only Bob can read the file. [2]

---

4 Go further

- work through the **5.4 Asymmetric Cryptography** lesson on the **Learn** page;
- read the **Securing Applications and Data** section of the AP Cybersecurity handout on the **Know** page.

Solutions

2.1 the recipient's public key.

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

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

3.1 A. encrypt with the recipient's public key.

3.2 B. RSA is asymmetric; AES is symmetric.

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