AP CYBERSECURITY • EXERCISE SHEET

5.3 Protecting Stored Data with Cryptography

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

KEY WORDS symmetric encryption 对称加密 • keyspace 密钥空间 • aes 高级加密标准 • ciphertext 密文 • block cipher 分组密码

Objective

Build the skills to answer exam questions on **symmetric encryption** 对称加密, keys, and **keyspace** 密钥空间.

You must be able to:

- define plaintext, ciphertext, key, and keyspace
- explain that symmetric encryption uses one shared key (e.g. **AES** 高级加密标准)
- relate key length to keyspace size (2^n)

1 Worked examples

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

■ The vocabulary

Encryption combines plaintext with a key to make ciphertext; decryption reverses it. The keyspace is the number of possible keys; an n-bit key has 2^n of them.

■ Symmetric encryption

Symmetric encryption uses the same key to encrypt and decrypt. AES is the standard block cipher. The challenge is sharing the single secret key safely.

2 Practice

2.1 Define **ciphertext**. [1]

2.2 Explain what 'symmetric' means in symmetric encryption. [2]

2.3 How many possible keys does a 4-bit key have? [1]

3 Exam-style questions

3.1 The standard modern symmetric block cipher is [1]

- **A** RSA
- **B** AES
- **C** HTTP
- **D** MAC

3.2 A larger keyspace makes an encryption key [1]

- **A** easier to guess
- **B** harder to guess
- **C** shorter
- **D** unnecessary

3.3 A company encrypts stored files with a symmetric algorithm.

(a) State the main practical challenge of symmetric encryption. [1]

(b) Explain why longer keys are more secure but slower. [2]

Solutions

2.1 the scrambled output of an encryption algorithm.

2.2 the same key is used to encrypt and to decrypt; both parties must share that secret key.

2.3 $2^4 = 16$.

3.1 B. AES is the symmetric standard.

3.2 B. more possible keys means more guessing time.

3.3 (a) sharing the single secret key safely. (b) a longer key has a larger keyspace so it is harder to guess, but it takes more time to encrypt and decrypt.