Exercise walk-through

Protecting Stored Data with Cryptography ▪ 5.3

eXercise

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)

Method — 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.

Method — 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.

Practice 2.1 ▪ 1 mark

Define **ciphertext**.

Solution 2.1

Worked steps

the scrambled output of an encryption algorithm B1.

Practice 2.2 ▪ 2 marks

Explain what ‘symmetric’ means in symmetric encryption.

Solution 2.2

Method: Symmetric encryption

Worked steps

the same key is used to encrypt and to decrypt B1; both parties must share that secret key B1.

Practice 2.3 ▪ 1 mark

How many possible keys does a 4-bit key have?

Solution 2.3

Method: The vocabulary

Worked steps

$2^4 = 16$ B1.

Exam-style 3.1 ▪ 1 mark

The standard modern symmetric block cipher is

A RSA

B AES

C HTTP

D MAC

Solution 3.1

Method: Symmetric encryption

A RSA

B AES ✓

C HTTP

D MAC

Worked steps

B. AES is the symmetric standard.

Exam-style 3.2 ▪ 1 mark

A larger keyspace makes an encryption key

A easier to guess

B harder to guess

C shorter

D unnecessary

Solution 3.2

Method: The vocabulary

A easier to guess

B harder to guess ✓

C shorter

D unnecessary

Worked steps

B. more possible keys means more guessing time.

Exam-style 3.3 ▪ 1 mark

A company encrypts stored files with a symmetric algorithm.
(a) State the main practical challenge of symmetric encryption.
(b) Explain why longer keys are more secure but slower.

Solution 3.3

Method: Symmetric encryption

Worked steps

(a) sharing the single secret key safely B1. (b) a longer key has a larger keyspace so it is harder to guess B1, but it takes more time to encrypt and decrypt B1.