AP CYBERSECURITY • EXERCISE SHEET

4.2 Authentication

Name: _____ Class: _____ Date: _____ **Total: 12 marks**

Objective

Build the skills to answer exam questions on **hashing** 散列, **salt** 盐值, password attacks, and authentication factors.

You must be able to:

- state the properties of a cryptographic hash (one-way, fixed length, repeatable)
- explain how salt protects stored passwords
- classify authentication factors (know / have / are / where) and password attacks

1 Worked examples

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

■ Hashing and salt

A service stores the hash of a password, never the plaintext. Salt (random bits) is added before hashing so two identical passwords produce different stored hashes.

■ Password attacks

Password spraying = one common password against many accounts. Credential stuffing = stolen or default credentials. A rainbow table = a precomputed table of passwords and their hashes.

2 Practice

2.1 State two properties of a cryptographic hash function. [2]

2.2 Explain how **salt** protects stored passwords. [2]

2.3 Classify each authentication factor as know / have / are / where.

(a) A fingerprint [1]

(b) A code sent to your phone [1]

(c) A PIN [1]

3 Exam-style questions

3.1 A cryptographic hash output is [1]

- **A** variable length
- **B** a fixed length regardless of input
- **C** the original password
- **D** always longer than the input

3.2 Trying one common password against many accounts is [1]

- **A** credential stuffing
- **B** password spraying
- **C** salting
- **D** a rainbow table

3.3 A company enables multifactor authentication (MFA).

(a) State what MFA requires. [1]

(b) Explain why it is stronger than a password alone. [2]

4 Go further

- work through the **4.2 Authentication** lesson on the **Learn** page;
- read the **Securing Devices** section of the AP Cybersecurity handout on the **Know** page.

Solutions

2.1 any two of: one-way/cannot reverse; fixed-length output; repeatable/same input same output.

2.2 salt adds unique random bits before hashing, so two identical passwords have different stored hashes.

2.3 (a) are / biometric. (b) have. (c) know.

3.1 B. a hash is fixed length and one-way.

3.2 B. one password, many users = password spraying.

3.3 (a) two or more different authentication factors. (b) an adversary must defeat two factors, so a stolen password alone cannot log in.