1.3 EXCHANGING DATA · 1.3.1

Encryption & hashing

Original practice questions · 30 marks · about 45 minutes · spec 1.3.1(c)(d)

Instructions. Answer all questions. The number of marks is shown in brackets [ ]. Quality of written communication is assessed in the extended-response question.

1

Total: 4 marks

This question is about encryption.

(a) State the purpose of encryption. **[1]**

(b) State the names of the two forms of data before and after encryption. **[2]**

(c) State whether encryption is a one-way or a two-way process. **[1]**

2

Total: 6 marks

This question is about symmetric and asymmetric encryption.

(a) Describe how symmetric encryption works. **[2]**

(b) Explain one drawback of symmetric encryption. **[2]**

(c) Explain how asymmetric encryption overcomes this drawback. **[2]**

3 **Total: 6 marks**

A website stores its users' passwords as hashes.

(a) Describe what is meant by a *hash*. **[2]**

(b) Describe one advantage of storing passwords as hashes rather than as plaintext. **[2]**

(c) Describe how the website can check a user's password at login without storing the password itself. **[2]**

4 **Total: 5 marks**

(a) State **two** uses of hashing other than storing passwords. **[2]**

(b) Explain **two** characteristics to look for in a good hashing algorithm. **[3]**

5 **Total: 9 marks**

A delivery robot stores some data on the robot itself and sends other data wirelessly back to a control centre. The developers must keep stored passwords safe and keep transmitted data confidential.

Compare the robot's use of encryption and hashing, explaining which is appropriate for storing passwords and which for keeping transmitted data confidential, and justify your answer. **[9]**

END OF QUESTIONS