Data Transmission

2.3 Symmetric and asymmetric encryption

Marking Scheme

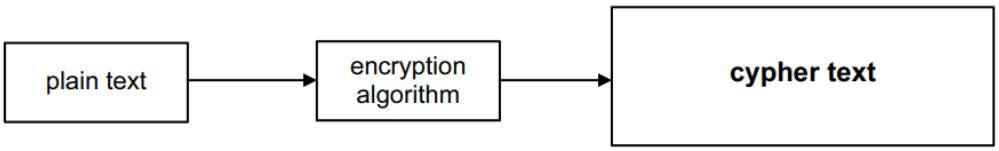
Q1)

(a) Any **one** from:
- jumbling up/scrambling characters so that message makes no sense
- requires an encryption key to encrypt data
- need decryption key to decipher encrypted message

[1]

(b) Uses the same key to encrypt and decrypt message [1]

(c) 1 mark for correct name in box



[1]

Q2)

symmetric encryption

encryption key

plain text

encryption algorithm

cypher text [5]

Question	Answer	Marks
3(a)	Any **four** from: – Encryption key is used – Encryption algorithm is used – Encryption key / algorithm is applied to plain text – … to convert it into cypher text – Same key is used to encrypt and decrypt the text	**4**
3(b)	Any **three** from: – Firewall – Password – Proxy server – Physical methods (by example e.g. CCTV, Locks) – Access rights – Asymmetric encryption – Disconnect from network	**3**

Question	Answer	Marks
4(a)	∞ a v m v e q n d i z m h (2 marks, 1 for each correct word)	2
4(b)	v w x y z a b c d e f g h i j k l m n o p q r s t u **2** marks ∞ shift right ∞ all characters shifted five places	2
4(c)	∞ the first cypher ∞ cannot deduce rest of cypher having identified some characters/more random substitution	2

Q5)

Question	Answer	Marks
	One mark for each correct term in the correct place. • plain text • cipher text • public key • private key	4

Q6)

(c)(i)	Data is **encrypted** and **decrypted** using the **same** key (1 mark) Any **three** from: • Plain text is encrypted into cipher text // cipher text is decrypted into plain text • **Data** is encrypted using an **algorithm** … • … that uses a key • The **key** can be generated using an **algorithm** • The **key** is **transmitted** to the receiver	4
(c)(ii)	Any **one** from: • To help keep the data secure • To make the data meaningless	1