1.3.1 Encryption

1. Jake wants to send a message over a network and decides to use asymmetric encryption.

a) State the purpose of encrypting data prior to transmission.

[1 mark]

- **To prevent intercepted data making sense / being intelligible to unauthorised users**

b) Explain how asymmetric encryption works, including the role of the public key and the private key

[4 marks]

- **The public key is applied to the data to encrypt it**
- **The public key is available to anyone who wants to encrypt data for a specific recipient**
- **The private key is used to decrypt the data**
- **Only the recipient has access to their private key**

2. The XOR operator can be used to encrypt data.

a) Show the effect of applying XOR on Text and Key, by completing the last row of the table below.

Text	O								C								R							
Value	0	1	0	0	1	1	1	1	0	1	0	0	0	0	1	1	0	1	0	1	0	0	1	0
Key	A								B								C							
Value	0	1	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0	1	0	0	0	0	1	1
XOR	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**1**

[2 marks]

b) Show the effect of applying XOR on Text and Key, by completing the last row of the table below.

(a)	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**1**
Key	A								B								C							
Value	0	1	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0	1	0	0	0	0	1	1
XOR	**0**	**1**	**0**	**0**	**1**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**

[2 marks]

c) Explain whether the type of encryption described above is symmetric or asymmetric.

[2 marks]

- **Symmetric**
- **… as the same key is used to encrypt and decrypt the data**