IGCSE Computer Science: **s25 11**

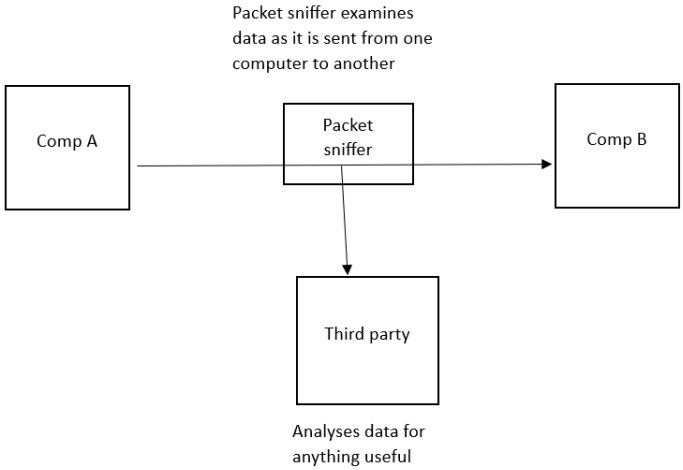
6(a)	**One** mark for each correct term in the correct position • algorithm • plain text • cipher text • meaningless • public/private • private/public (must be opposite of MP5) • public • private Data is encrypted using an encryption key. This is a type of **algorithm** that scrambles the **plain text** and turns it into **cipher text**. This makes the data **meaningless**. A **public/private** key is used to encrypt the data. This key cannot be used to decrypt the data. A **private/public** key is used to decrypt the data. Any device is able to request the **public** key, but only your device knows the **private** key.
6(b)	Any **one** from: • The process is more secure. • Do not need to worry about key exchange.

IGCSE Computer Science: **s24 11**

7	**One** mark for each correct term in the correct place. • plain text • cipher text • public key • private key

IGCSE Computer Science: **m24 12**

7(a)(i)	If the data is intercepted, it cannot be understood
7(a)(ii)	**Four** from: • Symmetric has a shared key… • … to encrypt **and** decrypt • Both the sender and receiver know the key • Asymmetric has different keys // a public key **and** a private key • …public to encrypt the data **and** private to decrypt • …anyone can know the public key but only those intended know the private key
7(b)(i)	Any **two** from: e.g. • Destination address/IP • Sender address/IP • Packet number
7(b)(ii)	Any **one** from: • Control the route the packet takes • Send each packet towards its destination • Choose more efficient route

8(a)	The diagram demonstrates (**One** mark for each part of the diagram): – Data is being sent from one device to another – The data is being examined **during transmission** – Packet sniffer is used – Intercepted data is reported to a third-party **during transmission** … – … and analysed for anything useful – Connection hacked to spoof destination address e.g. 
8(b)	– Encryption … – … if the data is intercepted it will be **meaningless** (because they do not have the decryption key)