SMART EXAM RESOURCES

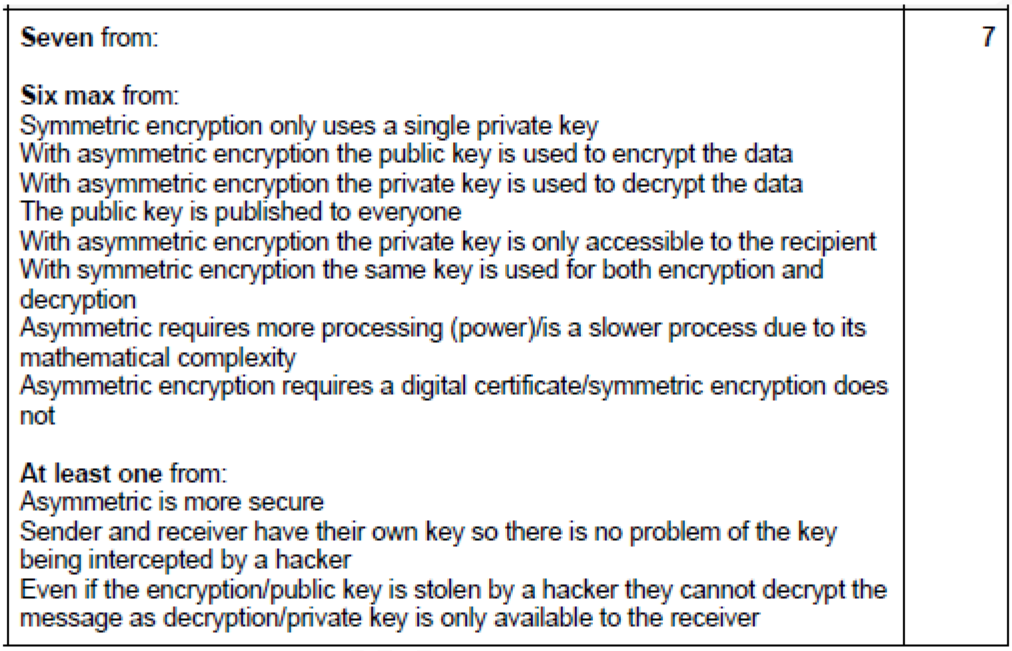
9626-INFORMATION AND COMMUNICATION TECHNOLOGY

TOPIC MARK SCHEMES

TOPIC: UNIT 1. 3 ENCRYPTION

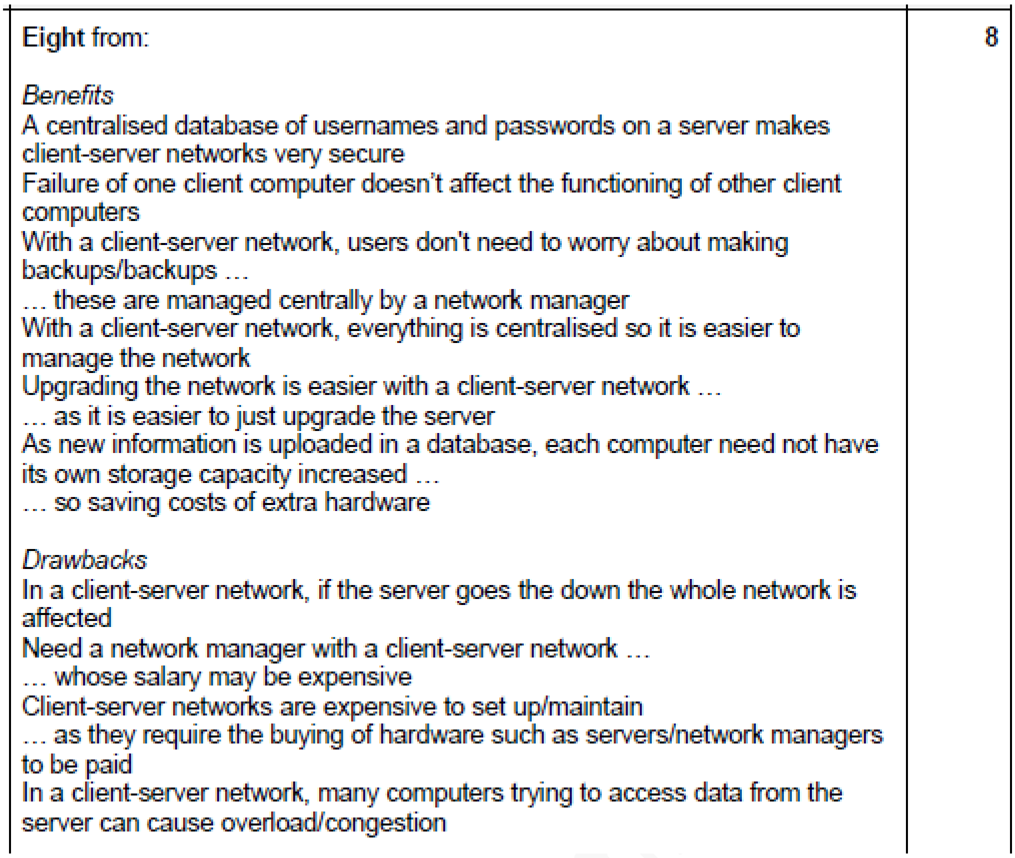
PAPER-1 SET-2

MARK SCHEME 1



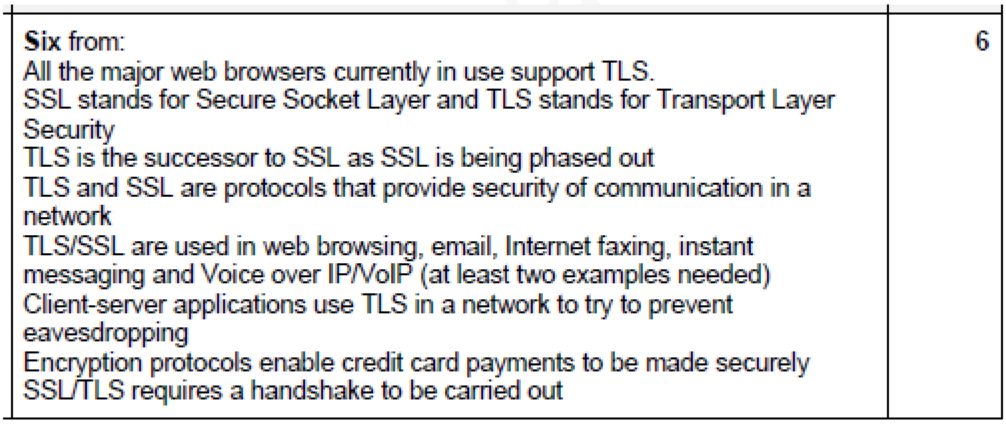
Seven from: **Six max** from: Symmetric encryption only uses a single private key With asymmetric encryption the public key is used to encrypt the data With asymmetric encryption the private key is used to decrypt the data The public key is published to everyone With asymmetric encryption the private key is only accessible to the recipient With symmetric encryption the same key is used for both encryption and decryption Asymmetric requires more processing (power)/is a slower process due to its mathematical complexity Asymmetric encryption requires a digital certificate/symmetric encryption does not **At least one** from: Asymmetric is more secure Sender and receiver have their own key so there is no problem of the key being intercepted by a hacker Even if the encryption/public key is stolen by a hacker they cannot decrypt the message as decryption/private key is only available to the receiver	7

MARK SCHEME 2



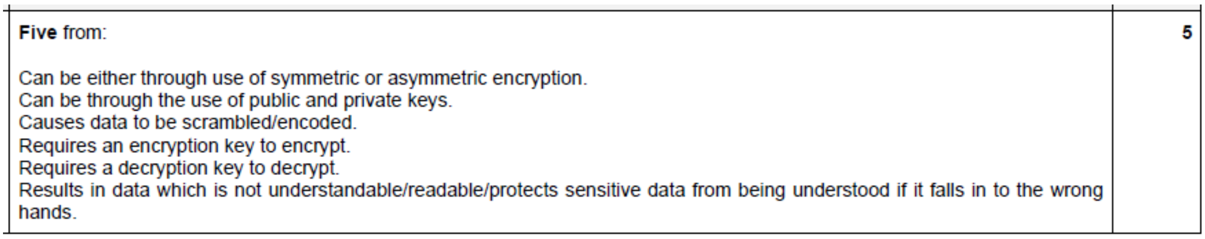
Eight from: *Benefits* A centralised database of usernames and passwords on a server makes client-server networks very secure Failure of one client computer doesn't affect the functioning of other client computers With a client-server network, users don't need to worry about making backups/backups … … these are managed centrally by a network manager With a client-server network, everything is centralised so it is easier to manage the network Upgrading the network is easier with a client-server network … … as it is easier to just upgrade the server As new information is uploaded in a database, each computer need not have its own storage capacity increased … … so saving costs of extra hardware *Drawbacks* In a client-server network, if the server goes the down the whole network is affected Need a network manager with a client-server network … … whose salary may be expensive Client-server networks are expensive to set up/maintain … as they require the buying of hardware such as servers/network managers to be paid In a client-server network, many computers trying to access data from the server can cause overload/congestion	**8**

MARK SCHEME 3



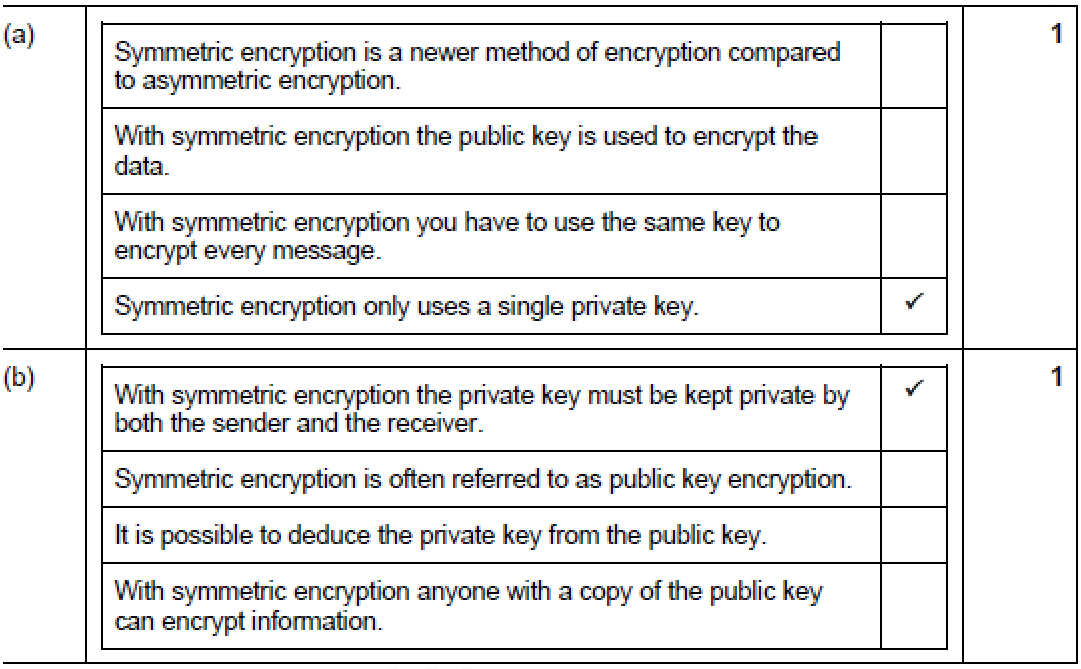
Six from: All the major web browsers currently in use support TLS. SSL stands for Secure Socket Layer and TLS stands for Transport Layer Security TLS is the successor to SSL as SSL is being phased out TLS and SSL are protocols that provide security of communication in a network TLS/SSL are used in web browsing, email, Internet faxing, instant messaging and Voice over IP/VoIP (at least two examples needed) Client-server applications use TLS in a network to try to prevent eavesdropping Encryption protocols enable credit card payments to be made securely SSL/TLS requires a handshake to be carried out	**6**

MARK SCHEME 4



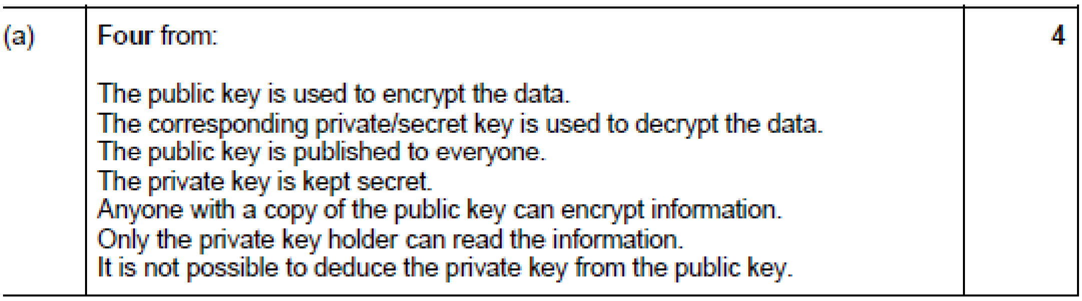
Five from: Can be either through use of symmetric or asymmetric encryption. Can be through the use of public and private keys. Causes data to be scrambled/encoded. Requires an encryption key to encrypt. Requires a decryption key to decrypt. Results in data which is not understandable/readable/protects sensitive data from being understood if it falls in to the wrong hands.	**5**

MARK SCHEME 5

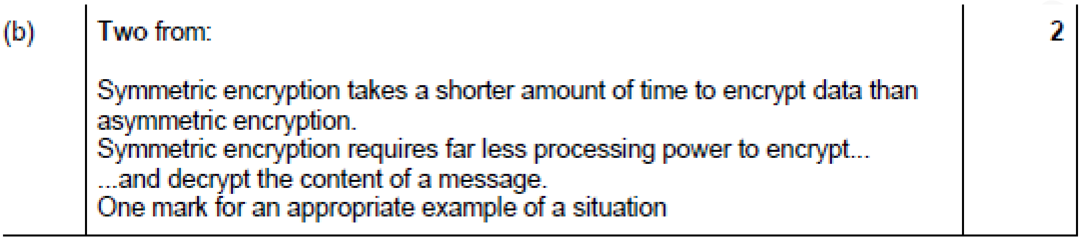


(a)	Symmetric encryption is a newer method of encryption compared to asymmetric encryption.		**1**
	With symmetric encryption the public key is used to encrypt the data.		
	With symmetric encryption you have to use the same key to encrypt every message.		
	Symmetric encryption only uses a single private key.	✓	
(b)	With symmetric encryption the private key must be kept private by both the sender and the receiver.	✓	**1**
	Symmetric encryption is often referred to as public key encryption.		
	It is possible to deduce the private key from the public key.		
	With symmetric encryption anyone with a copy of the public key can encrypt information.		

MARK SCHEME 6



(a)	Four from: The public key is used to encrypt the data. The corresponding private/secret key is used to decrypt the data. The public key is published to everyone. The private key is kept secret. Anyone with a copy of the public key can encrypt information. Only the private key holder can read the information. It is not possible to deduce the private key from the public key.	4



(b)	Two from: Symmetric encryption takes a shorter amount of time to encrypt data than asymmetric encryption. Symmetric encryption requires far less processing power to encrypt... ...and decrypt the content of a message. One mark for an appropriate example of a situation	2