SMART EXAM RESOURCES

9626-INFORMATION AND COMMUNICATION TECHNOLOGY

TOPIC MARK SCHEMES

TOPIC: UNIT 1. 3 ENCRYPTION

PAPER-1 SET-1

MARK SCHEME 1

Eight from: Encryption is the scrambling of data… …it converts plaintext to ciphertext... …into meaningless groups of symbols… … can't be understood by unauthorised people/read without the decryption key… …without encryption messages can be stored as plain text, making it easy for anyone to read and understand Encryption keeps personal data secure… … …such as credit card numbers and personal information from computer hackers If personal information is intercepted, but it can't be understood, it is of no use... ... the act of hacking in this case is pointless It does not prevent hackers intercepting personal data but it prevents them from understanding it Two types of encryption asymmetric and symmetric… …symmetric and asymmetric use a private key but asymmetric uses a public key as well /symmetric uses the same key to encrypt and decrypt but asymmetric uses different keys… …symmetric uses a private key to encrypt and decrypt /symmetric is where both sender and receiver use a private key… …asymmetric uses a public key to encrypt and a private key to decrypt /sender uses a public key and receiver uses a private key Can only decrypt using a decryption key/only authorised users have the decryption key… … Symmetric is a faster method than asymmetric… … Symmetric is less secure than asymmetric Data is encrypted using an encryption key **Must be a proper analysis to gain full marks** **Max. six marks if bullets/list of points** **Must have expansions to be a proper analysis**	8

MARK SCHEME 2

Four from: When a file is written to the disk, it can be automatically encrypted by encryption software Full disk encryption is when the data is encrypted as soon as it is saved to the hard disk When a file is read from the disk the decryption/encryption key/password is needed to decrypt it When a file is read from the disk, the software automatically decrypts it… … while in some types of hard disk encryption leaving all other data on the disk encrypted (All) the files on the disk are encrypted/ It's the encryption of data on that disk… …except in some cases the operating system Whether the disk stays in the computer or moved to another computer it is still encrypted Only the person/computer with the secret/decryption/encryption key/password can understand the data on the disk/data can't be read without the decryption/encryption key/unauthorised people cannot read the data	**4**

MARK SCHEME 3

Six from: Transport Layer Security (TLS) is used for applications that require data to be securely exchanged over a client-server network... ...such as web browsing sessions/ file transfers The server shows/sends its SSL/TLS/digital certificate to the client /the client requests server's SSL/TLS/digital certificate To open a SSL/TLS connection, a client needs to obtain the public key The public key is found in the server's digital certificate The SSL/TLS/digital certificate authenticates the server to the client/identifies the server The client then carries out a number of checks to make sure that the certificate was issued by a trusted CA… …is in date and that the server is the legitimate owner of the public and private keys For the client to access the server the client and server must carry out a SSL/TLS handshake… …the client tells the server what version of SSL/TLS it uses… …and a list of the different types of encryption that it is able to use The client tells the server that it wants to set up a communications channel Handshaking occurs before the transfer of data can take place The server tells the client the type of encryption it has chosen from the client's list	**6**

MARK SCHEME 4

Five from: • Often called public-key encryption (1) • Uses two **different** keys// one public and one private/secret (key) (1) • No need to transfer a key (with the message) (1) • The **public** key/key held by **the person doing the encryption** is used to encrypt the data (1) • The corresponding **private/secret** key is used to decrypt the data (1) • The **public** key is published to everyone (1) • The **private** key is kept secret (1) • **Anyone** with a copy of the **public key** can encrypt information (1) • **Only** the **private key** holder can read the information (1) • It is not possible to deduce the private key from the public key (1)	**5**

MARK SCHEME 5

l(a)	**Four** from: • When a message/information is intercepted//accessed **it is unreadable/ can't be understood** ... (1) ... so, therefore, it is **useless** (1) ... to a hacker (accept alternative examples of 3rd party or just 'third party') (1) • It protects customers when they bank/shop online/any other suitable example from any area of use (MUST BE protecting data) ... (1) ... as the data cannot be used for identity theft (1) • Data can only be decrypted by the receiving computer if it has the private/decryption key (1) **Max. three marks if bullets/list of points**	**4**

l(b)	**Up to FOUR marks available:** ***Advantages (MAX 3)*** • It is a faster process//quicker **to encrypt compared to asymmetric** (1) ... ... as it has less mathematical complexity (1) • It requires less computational power **than asymmetric** (1) ***Disadvantages (MAX 3)*** • Does not have a different key for encryption and decryption//sender and receiver use the same key (1) ... ... therefore only one key needs to be stolen (1) ... making it less secure (1) • The encryption key cannot be generally published (1) • The encryption key must be sent to the receiver of the message (1) • Key could be intercepted/stolen (by a hacker) **whilst being sent** ... (1) ... who can then decrypt any message encrypted by the sender (accept any reasonable implication) (1) **Must have at least one of each to gain full marks** **Max. three marks if bullets/list of points**	**4**

MARK SCHEME 6

Eight from: *Advantages* Account details cannot be read by another user … … unless they possess appropriate permissions As modern technology becomes more sophisticated, so do hackers … … so taking security precautions is essential Passwords to access accounts are not enough Without encryption a person/malware could potentially see someone else's account details Does not matter which device (mobile phone/computer) is being used; data is encrypted Reassures bank customers that their data is secure *Disadvantages* If the password is lost or reset, it becomes impossible to gain information from the account Encryption uses a lot of server resources … … requiring processing power and memory In some circumstances it can cause delays in accessing bank's web site Need to buy an SSL certificate … … issued by certificate authorities Encryption means the systems that maintain data encryption must have capacity and upgrades… … which can be quite costly	8