MODULE D DATA TRANSMISSION · D6

Encryption: mark scheme

20 marks · OCR J277 spec 1.3.2, 1.4.2, 1.5.2

How to use. 1 mark per bullet up to the maximum shown. **/** separates alternative words; **//** separates alternative statements for the same mark. Words in (brackets) are not needed for the mark. J277 tests the **principle** of encryption only: symmetric and asymmetric encryption are not on the J277 specification and are not needed for any mark here (credit a correct mention, but it earns nothing extra).

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.3.2	(The data is) scrambled / encoded using an (encryption) algorithm // using a key (So it is) meaningless / cannot be understood without the key	**2**	1 mark per bullet. Accept "turned into ciphertext" for bullet 1 (not required). "Cannot be read / accessed" alone = NE (it can be read, it just cannot be understood). Do not award "it cannot be intercepted".
1(b) J277 1.3.2	The key	**1**	2+ ticks = 0.
2(a) J277 1.3.2	The plans are scrambled / encoded (before being sent) ... using an (encryption) algorithm / a key If the plans are intercepted (e.g. on the public Wi-Fi) they are meaningless / cannot be understood Only the client / someone with the (correct) key can decrypt them / turn them back into the original plans	**3**	1 mark per bullet, max 3. "It keeps them safe" / "it locks them" = NE. "Cannot be read / accessed" alone = NE (it can be read, it just cannot be understood). Do not award "stops the plans being intercepted / stolen" (a wrong statement; see 2(b)).
2(b) J277 1.3.2, 1.4.2	Encryption does not stop data being intercepted // the plans can still be intercepted / copied ... but the intercepted data cannot be understood / is meaningless (without the key)	**2**	1 mark per bullet. Second mark depends on the first idea being present or clearly implied. "Hackers can break encryption" alone = 0 (does not explain the misunderstanding).

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) J277 1.3.2, 1.4.2, 1.5.2	Row 1: True Row 2: False Row 3: True Row 4: False	**4**	1 mark per correct row. 2 ticks in a row = 0 for that row. Row 2: limiting malware is anti-malware software's job. Row 4: reducing file size is compression, not encryption.
4(a) J277 1.4.1, 1.4.2	Data interception (and theft)	**1**	Accept "interception" / "someone intercepting the data" / "data theft". Do not accept hacking (NE), malware, phishing, brute-force, DoS.
4(b) J277 1.4.2	The names and addresses are scrambled / converted into ciphertext (using a key) If intercepted / stolen, the data is meaningless / cannot be understood ... without the (correct) key // only head office (with the key) can decrypt it	**2**	1 mark per bullet, max 2. "Cannot be read / accessed" alone = NE (it can be read, it just cannot be understood). Do not award "stops the data being intercepted".
5(a) J277 1.5.2	To scramble / encode data (stored on the device) so it cannot be understood without the key // to protect stored data from being read by unauthorised people	**1**	"To keep files secure" alone = NE.
5(b) J277 1.5.2, 1.4.2	The files on the laptop are stored encrypted / as ciphertext The person who took it cannot understand the files // the files are meaningless to them ... because they do not have the key	**2**	1 mark per bullet, max 2. "Cannot be read / accessed" alone = NE (it can be read, it just cannot be understood). Must be in context of the stolen laptop / files. Do not award "the laptop cannot be stolen" or "the files are deleted".
6(a) J277 1.3.2	Passwords / login details Bank / payment card details // online payments Personal data, e.g. names, addresses, medical records Private messages / emails Data sent to / from a secure website (HTTPS) Data sent over Wi-Fi Confidential business data, e.g. plans, contracts	**2**	1 mark each, max 2. Mark the first answer on each line. Two answers that are the same idea (e.g. "names" and "addresses") = 1 mark. Accept any other sensible confidential data. "Data" / "files" alone = NE.

Total: 20 marks