MODULE D DATA TRANSMISSION · D6

Encryption: mark scheme

21 marks · Cambridge 0478 syllabus 2.3.1, 2.3.2

How to use. One mark per creditworthy point up to the maximum shown. **/** separates alternative words; **//** separates alternative answers. Words in (brackets) are not needed for the mark. Marked positively: no deductions.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 2.3.1	Any one from: • so that if the data is intercepted it cannot be understood / is meaningless • to keep personal / confidential data private // so only the warehouse (with the key) can read it • to protect against data theft / misuse of the details	**1**	"To keep it safe / secure" alone = TV. Do not accept "to stop it being intercepted".
1(b) 0478 2.3.1, 2.3.2	cipher text // ciphertext	**1**	Do not accept "encrypted data" (repeats the question) or "scrambled".
1(c) 0478 2.3.1	Any two from: • encryption does not prevent the data being intercepted / copied (as it is transmitted) • the data is scrambled / is cipher text, so an interceptor cannot understand it • it cannot be decrypted without the (correct) key	**2**	max 2.
2(a) 0478 2.3.2	One mark for each correct word, in order: plain algorithm cipher same sent	**5**	Distractors: different, intercepted, private. Gap 5: accept "given / transmitted / shared" (correct meaning) though not in the list.
3(a) 0478 2.3.2	(The printing company's) public key	**1**	Do not accept "the design agency's public key" or any private key.
3(b) 0478 2.3.2	(The printing company's) private key	**1**	Must be the opposite of 3(a). Do not accept "the design agency's private key".

QUESTION	ANSWER	MARKS	GUIDANCE
3(c) 0478 2.3.2	Any two from: • the public key can only be used to encrypt (the data) // cannot be used to decrypt the data • only the (matching) private key can decrypt the drawings • the private key is kept by the printing company / is never sent / shared	**2**	max 2. "The public key is meant to be public" alone = TV.
4(a) 0478 2.3.2	One mark for each correct row: Row 1: Asymmetric Row 2: Both Row 3: Symmetric Row 4: Asymmetric	**4**	More than one tick in a row = 0 for that row. Row 4: the private key stays with the receiver.
5(a) 0478 2.3.2	Any four from: • two (different but matching) keys are used: a public key and a private key • the partner office (receiver) sends / shares its public key with the firm // the public key is available to anyone • the firm encrypts the records with the partner office's public key • (using an encryption algorithm) the plain text is turned into cipher text • the cipher text is transmitted to the partner office • the partner office decrypts the records with its (matching) private key • the private key is kept secret / is never transmitted	**4**	max 4. Do not credit a reversed answer (encrypt with private, decrypt with public), or keys belonging to the wrong organisation (e.g. "the firm's public key").

Total: 21 marks