Making IT
good for society

BCS Level 4 Certificate in Employment of Cryptography
Answer Key and Rationale QAN 603/0892/8

Question	Answer	Explanation / Rationale	Syllabus Sections
1	**D**	IPsec includes AH (The Security Authentication Header), ESP (Encapsulating Security Payload) and SA (Security Authentications).	1.3
2	**D**	Client Authentication uses a certificate to authenticate a user.	2.1
3	**C**	A feature of digital signatures is non-repudiation, meaning that the signer cannot deny signing a message. The other responses are features of cryptography that do not directly provide non-repudiation.	1.3
4	**D**	A collision attack on a hash function, such as MD5, attempts to find two different messages that will produce the same hash.	1.4
5	**C**	Entropy from various sources is used as an input to PRNG to generate keys that are needed on a periodic basis.	1.5
6	**B**	Simple substitution ciphers systematically replace each symbol in the message for another symbol, also called a one-to-one correspondence table.	1.1
7	**B**	In general, escrow is something (for example, a document or an encryption key) that is delivered to a third party and is to be given to the grantee only upon the fulfilment of a predefined condition. (for example, a grantor and grantee relationship with a third party in the middle)	3.1
8	**A**	This mechanism by using the signers private key and a hash function allows the receiver to identify both the sender and that it has not be tampered with during transit.	2.5
9	**C**	Digital signing ensures the integrity of patches and drivers.	2.5
10	**A**	Block ciphers encrypt blocks of data of a constant size. Polyalphabetic substitution ciphers change the substitution alphabet for every symbol. Transposition ciphers take groups of characters and shift them according to a regular system.	1.1
11	**A**	A5/2 is the cipher used to encrypt GSM cellular communication.	2.2

Question	Answer	Explanation / Rationale	Syllabus Sections
12	**A**	When using an open source, you are dependent on a service that may or may not have been tested to the standards you require.	2.3
13	**B**	In a block cipher, one cryptographic key and algorithm are applied to the entire block of data (e.g. 64 contiguous bits) at once as a group rather than to one bit at a time.	1.2
14	**D**	A block cipher uses symmetric cryptography and therefore an asymmetric key cipher mode could not be used. ECB, CFB, and CBC modes are all symmetric and can be used for a block cipher.	1.2
15	**C**	Keys are protected by the hardware of the Trusted Platform Module (TPM) where they are not reachable by the outside world through the Internet.	2.1
16	**B**	Padding Oracle On Downgraded Legacy Encryption (POODLE) attack is the down attack where a man-in-the-middle exploit takes advantage of Internet and security software clients' fall back to SSL 3.0.	2.3
17	**C**	Wassenaar Arrangement Export Control regime requires an export license. This is often considered as a bottleneck by the security responders. However, this clause is meant to ensure control of the information exchange by the authorities to distinguish between good and bad.	3.2
18	**B**	ISO 27001 is the standard that covers policy and regulation on the use of cryptographic controls. ISO 9001 is a quality management standard. Common criteria is used for the security evaluation; and ISO 17025 is for the testing facilities.	3.3
19	**B**	IDEA uses 128-bit key.	3.1
20	**A**	Only a full disk encryption can avoid data theft. The inventory of the devices will help keep a record of the devices during transportation. But in case any of the device is lost than the inventory list will not provide any protection for the data. Likewise, insurance policy will not protect against the loss of data. Shock absorbers provide physical protection only. They do not protect from data loss.	2.2