BCS Level 4 Certificate in Employment of Cryptography QAN 603/0892/8

Specimen Paper Answer Key

Version 4.0
July 2020

Change History

Any changes made to the specimen paper shall be clearly documented with a change history log. This shall include the latest version number, date of the amendment and changes made. The purpose is to identify quickly what changes have been made.

Version Number	Changes Made
Version 1.0 September 2017	Document created.
Version 2.0 September 2017	Amended to reflect syllabus following enhancement process.
Version 3.0 September 2018	Updated to link with 20-question paper.
Version 4.0 July 2020	Major changes to questions to match updated syllabus (V3.0). Title page, change history table and related syllabus section added.

Related Syllabus

This specimen paper and answer key are related to the following syllabus:

BCS Level 4 Certificate in Employment of Cryptography Syllabus V3.0 March 2020

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

Question	Answer	Explanation / Rationale	Syllabus Sections
1	**A**	PGP is technically an asymmetric form of encryption.	1.1
2	**D**	RC4 is the only stream cipher listed.	1.1
3	**D**	RSA is asymmetric. The other ciphers listed are symmetric.	1.1
4	**B**	SSL/TLS is the technology used for HTTPS.	1.2
5	**B**	A VPN is normally used to encrypt traffic on an open WiFi network.	1.2
6	**C**	Smart cards are typically used as a second factor of authentication - "something you have", in addition to "something you know", for example a password.	1.2
7	**B**	A brute force attack is where an attacker tries all possible password combinations to gain access to something that has been access protected.	1.3
8	**A**	This is the definition of a replay attack, re-sending encrypted traffic to try and impersonate the legitimate user.	1.3
9	**D**	Side-channel attack is based on information gained from the physical implementation of a cryptosystem e.g. timing information leakage. The other options rely on attacking the encrypted data.	1.3
10	**D**	DES is the only option listed that is obsolete. MD5 is not an encryption algorithm, and Twofish and PGP are not considered to be obsolete.	1.4
11	**C**	SHA1 is deprecated due to several implementation flaws that could result in attack.	1.4
12	**B**	A one-time password (OTP) device that has reached the end of its lifecycle would be destroyed.	1.5
13	**A**	Key escrow ensures access to private keys can be agreed in advance of generation.	1.5
14	**B**	This is a core limitation of using symmetric keys. Typically, symmetric keys are sent via an asymmetric encrypted "control" connection, or an out of band method.	1.6
15	**A**	Having a certificate authority is required to issue asymmetric keys in most instances.	1.6
16	**C**	Entropy from various sources is used as an input to generate session keys. The entropy or randomness ensures the keys are not easily guessable.	1.7
17	**D**	BitLocker is a technology primarily used for full disk encryption; the other options are not disk encryption technologies.	2.1
18	**D**	This is a key feature of WhatsApp and is the primary method of protecting data in transit.	2.1

Question	Answer	Explanation / Rationale	Syllabus Sections
19	**B**	Several countries in the world have import restrictions on cryptography and require vendors to have a license.	2.2
20	**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.	2.3