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

# Specimen Paper

## 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<br>September 2017 | Document created. |
| Version 2.0<br>September 2017 | Amended to reflect syllabus following enhancement process. |
| Version 3.0<br>September 2018 | Updated to link with 20-question paper. |
| Version 4.0<br>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 sample 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 QAN 603/0892/8

## Specimen Paper

Record your surname/ last/ family name and initials on the Answer Sheet.

**Specimen paper only. 20 multiple-choice questions** – 1 mark awarded to each question. Mark only one answer for each question. There are no trick questions.

A number of possible answers are given for each question, indicated by either A. B. C. or D. Your answers should be clearly indicated on the Answer Sheet.

The pass mark is 13/20.

This is a specimen examination paper only.



**This qualification is regulated by Ofqual (in England).**

**1** PGP is a form of what?

**A** Asymmetric encryption.
**B** Symmetric encryption.
**C** Elliptic curve cipher.
**D** Hashing algorithm.

**2** Which of the following encryption algorithms is a stream cipher?

**A** RC5.
**B** AES.
**C** PGP.
**D** RC4.

**3** Which of the following is an asymmetric cryptographic cipher?

**A** 3DES.
**B** AES.
**C** RC4.
**D** RSA.

**4** When visiting an e-commerce site, which of the following cryptographic technologies is **NORMALLY** used?

**A** BitLocker.
**B** SSL/TLS.
**C** WPA2.
**D** DRM.

**5** Which technology is **TYPICALLY** used to encrypt communications over a public wireless network?

**A** Telnet.
**B** VPN.
**C** TETRA.
**D** WEP.

**6** Smart cards are **TYPICALLY** used as a form of what?

**A** Cryptocurrency.
**B** Copy protection.
**C** Two-factor authentication.
**D** Document encryption.

**7** What is a brute force attack?

**A** Using zombies to send large amounts of network traffic.
**B** Trying all possible password combinations.
**C** Encrypting users' files and asking for a payment in return.
**D** Sniffing unencrypted packets with Wireshark.

**8** Which of the following is an example of a replay attack?

**A** Capturing a banking transaction and re-sending it at a later date.
**B** Logging into a website multiple times with many different passwords.
**C** Poisoning an ARP cache to impersonate a server.
**D** Monitoring a card reader for voltage fluctuations when a door is opened.

**9** What is an attack based on information gained from the physical implementation of a cryptosystem called?

**A** Sniffer attack.
**B** Brute-force-attack.
**C** Cryptanalytic attack.
**D** Side-channel attack.

**10** Which of the following encryption algorithms is obsolete?

**A** Twofish.
**B** MD5.
**C** PGP.
**D** DES.

**11** Which of the following hashing algorithms is no longer recommended?

**A** SHA2.
**B** AES128.
**C** SHA1.
**D** AES256.

**12** Which stage of key management is **TYPICALLY** associated with an OTP device that has expired and is no longer required?

**A** Revocation.
**B** Destruction.
**C** Regeneration.
**D** Redeployment.

**13** In the generation stage of the key lifecycle, there is a requirement that a third party may need access to the key. Which of the following **COULD** be implemented?

**A** Key escrow.
**B** Shared credentials.
**C** Intermediate CA.
**D** Pre-shared key.

**14** Which of the following is a limitation of using symmetric encryption?

**A** Symmetric keys are very resource intensive.
**B** Encryption keys must be communicated to both parties securely.
**C** Symmetric keys are not trusted by all browsers.
**D** A key revocation list must be implemented and tested.

**15** When managing keys, which of the following is **TYPICALLY** a limitation of using asymmetric encryption?

**A** The availability of a certificate authority.
**B** Sharing the private keys securely.
**C** A revocation process is not possible.
**D** Not supported for web browsing.

**16** Entropy in a computer system may be used for which of the following purposes?

**A** To detect intrusion attempts by their signature.
**B** To verify passwords at login.
**C** To create session keys.
**D** To scan attachments for threats.

**17** There is a business requirement to enable full disk encryption on all company PCs. Which of the following technologies **COULD** be used?

**A** Fingerprint scanner.
**B** Password manager.
**C** Two-factor authentication.
**D** BitLocker.

**18** A technologist sends confidential information over WhatsApp. Which of the following **PRIMARILY** prevents a third party from reading the message?

**A** Official App Store / Google Play app.
**B** Secure Hash Algorithm.
**C** A secure wireless network.
**D** End-to-end encryption.

**19** Which of the following is a **KEY** consideration when importing cryptography?

**A** Must use the latest algorithms.
**B** Import licenses.
**C** Contractual agreements.
**D** Written approval from the vendor.

**20** Which regulation requires cyber responders and security researchers to obtain an export license prior to exchanging essential information to fix a newly identified security vulnerability?

**A** General Data Protection Regulation.
**B** Sarbanes-Oxley Act.
**C** Wassenaar Arrangement Export Control regime.
**D** Data Protection Act.

**-End of Paper-**