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

Sample 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 September 2017	Document created.
Version 2.0 February 2018	Updates to questions.
Version 2.1 July 2018	Title corrected.
Version 3.0 October 2019	Updates to questions.
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 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

Sample Paper

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

Sample paper only. 40 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 26/40.

This is a sample 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.

21 Which of the following is a hashing algorithm?

A AES256.
B SHA256.
C 3DES.
D Diffie-Hellman.

22 What is a benefit of using an elliptic curve cipher over traditional ciphers?

A Encrypted message is longer.
B Keys are longer and more effective.
C Keys are shorter but just as effective.
D Encrypted message cannot be cracked.

23 Which of the following is a symmetric encryption algorithm?

A RSA.
B 3DES.
C Diffie-Hellman.
D DSA.

24 Which of the following ensures that passwords are not stored in plain text?

A Certificate authority.
B Blockchain.
C Hashing.
D Message signing.

25 Product keys are **TYPICALLY** used for what?

A Full disk encryption. Protecting the contents of a hard drive.
B Cryptocurrency. Sending and receiving bitcoins securely.
C User authentication. Verifying the user is who they say they are.
D Digital rights management. Ensuring software is only used by an authorised party.

26 Which of the following can be used on a set of external storage devices to protect against sensitive data theft if the devices are used for the data transfer from a remote location to the company's data warehouse?

A Full disk encryption of each device.
B Inventory of the devices including their serial numbers.
C Copy of the third-party insurance policy detailing clauses of equipment lost.
D Place each device in a shock absorber.

27 A technologist opens a web browser and accesses https://www.facebook.com. A warning message appears on screen, with an option to continue. Which of the following **COULD** be happening?

A Man-in-the-middle attack.
B Brute force attack.
C Replay attack.
D Pass-the-hash attack.

28 Which of the following would be deemed a key theft attack?

A Theft of a public key.
B Theft of a certificate authority.
C Theft of an SSL certificate.
D Theft of a private key.

29 A technologist discovers rogue devices connected to their encrypted wireless network. Which crypto system is **MOST LIKELY** to be in use?

A WEP.
B WPA2-Personal.
C WPA2-Enterprise.
D 3DES.

30 A technologist implements an IPSec tunnel using AES128 and MD5. Which of the following may occur?

A Handshake failure when the tunnel is established.
B Breach of integrity due to an obsolete algorithm.
C Older hardware may not support the latest algorithms.
D Breach of confidentiality due to an obsolete encryption algorithm.

31 In key management, a technologist discovers their private key has been stolen. What is the **first** step to remediate the breach?

A Generation.
B Destruction.
C Revocation.
D Deployment.

32 Which of the following is a **PRIMARY** stage of key lifecycle management?

A Generation.
B Timeframe.
C Encryption.
D Decryption.

33 Which of the following is **TYPICALLY** required for self-signed certificate generation?

A Intermediate Certificate Authority.
B Master Certificate Authority.
C Certificate Authority.
D Primary Certificate Authority.

34 When managing private keys as part of an asymmetric cryptosystem, which of the following must apply?

A Ensuring the keys are sent to a third party securely.
B Ensuring the keys are not shared with any third party.
C Ensuring the key length is at least 128 bits.
D Ensuring the revocation list is working correctly.

35 What is the **MOST LIKELY** benefit of using a cloud-based key management service?

A More scalable than an on-premise solution.
B Access to the latest encryption algorithms.
C More secure than an on-premise solution.
D Integration with a password manager.

36 In cryptography, which of the following is a benefit of entropy?

A Not CPU intensive.
B Open source.
C Faster encryption.
D Unpredictable.

37 When using a password manager, which of the following is **KEY** to keeping credentials secure?

A Using several password managers at once.
B Ensuring the password manager is regularly updated.
C Testing key revocation.
D A strong master password.

38 Which of the following encryption techniques is **TYPICALLY** used for processing bank transactions online?

A Transport Layer Security.
B Secure Sockets Layer.
C Message Digest 5.
D Out of band authentication.

39 A technologist has been asked to implement two-factor authentication (2FA) on a password protected system. Which of the following **BEST** achieves this?

A Password manager.
B Message signing.
C Authentication token.
D PIN number.

40 Which of the following is the **KEY** consideration when exporting cryptographic technology?

A Secure delivery.
B Licensing agreements.
C Legal implications.
D Compatibility.

-End of Paper-