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

## Sample Paper A

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

**1** Select the protocol suite that employs the following three protocols?

a) Authentication Headers (AH).
b) Encapsulating Security Payload (ESP).
c) Security Associations (SAs).

**A** HTTPS.
**B** TLS / SSL.
**C** SSH.
**D** IPsec.

**2** Which of the following statements **BEST** describes the goal of the Internet Key Exchange (IKE) for each of the two end points?

They independently produce...

**A** Different symmetrical keys before data is exchanged.
**B** The same symmetrical key before data is exchanged.
**C** The same symmetrical key and send it to the other party.
**D** A pair of asymmetrical keys before data is exchanged.

**3** Which of the following is a symmetric encryption algorithm?

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

**4** Non-repudiation is a feature of cryptography that can be implemented using which one of the following?

**A** VPN.
**B** IPSEC Tunnel.
**C** Digital Signature.
**D** Password Verification.

**5** A collision attack on MD5 attempts to find which of the following?

**A** Two messages that will produce two different hashes.
**B** One message that will produce two identical hashes.
**C** One message that will produce two different hashes.
**D** Two messages that will produce identical hashes.

**6** 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.

**7** A simple substitution cipher changes each plaintext symbol in what manner?

**A** It uses a different substitution alphabet for each symbol.
**B** It employs a one-to-one correspondence table.
**C** Plaintext is transformed into a group of random symbols.
**D** The cipher is changed into a single random symbol.

**8** Which of the following is **NOT** a secure VPN protocol?

**A** Internet Protocol Security (IPsec).
**B** Microsoft Windows Network Basic Input / Output System (NetBIOS).
**C** Transport Layer Security (SSL / TLS).
**D** Microsoft Secure Socket Tunnelling Protocol (SSTP).

**9** Which of the following describes a situation when a cryptographic key component is held by a third party?

**A** Key list.
**B** Key escrow.
**C** Key loader.
**D** Key exchange.

**10** A way of verifying both the sender of information and the integrity of a message is using which of the following?

**A** Digital signatures.
**B** Digital certificates.
**C** Public key encryption.
**D** Private key encryption.

**11** Why would a user check that a software patch is CORRECTLY signed by the software publisher?

**A** To ensure that the user does not exceed the software license.
**B** To ensure the patch downloaded correctly.
**C** To ensure that it is a legitimate patch issued by the correct party.
**D** To ensure the patch is compatible with the user's version of software.

**12** Which of the following is the CORRECT description of ciphers?

**A** Stream ciphers encrypt continuous streams of data.
**B** Block ciphers encrypt blocks of data of variable size.
**C** Polyalphabetic substitution ciphers keep the substitution alphabet constant for every symbol.
**D** Transposition ciphers take groups of characters and shift them according to a random system.

**13** Voice privacy in Global System for Mobile Communication (GSM) cellular telephone protocol is provided by which cipher?

**A** A5/2.
**B** B5/4.
**C** A6/2.
**D** B5/8.

**14** In the context of key management, which of the following is **NOT** an advantage of a 24-hour crypto period for the current key compared to a 30-day crypto period?

**A** If a key is compromised, there is less data to re-encrypt.
**B** Less data is exposed for any particular compromised key.
**C** As retired keys are deleted, there is less data for re-encryption.
**D** When a deleted key is retired, no data may be compromised.

**15** Which of the following is an organisation that sends out information about known security vulnerabilities in software?

**A** PGP.
**B** PKI.
**C** CERT.
**D** RSA.

**16** What is the downside of data cryptography on an open source?

**A** The data storage is dependent on a service that may have been poorly tested and possibly not work.
**B** Open source can create a sense of false security, it is cheaper and there is a community behind it.
**C** The data storage gets access to some extra flexibility, developers do not update often.
**D** Malicious users usually do not target open source so vulnerabilities are not found.

**17** Insecure HTTPS sessions can be caused by which of the following?

**A** Low entropy supplied to the pseudorandom number generator.
**B** Weak password hashing algorithms.
**C** Distributed denial-of-service (DDoS) attacks.
**D** Running unpatched application software.

**18** Which of the following can be provided by a digital signature for the message?

a) Confidentiality.
b) Integrity.
c) Authentication.
d) Nonrepudiation.

**A** b, c and d only.
**B** a, b and c only.
**C** a and b only.
**D** c and d only.

**19** Which of the following statements is TRUE, in a block cipher?

**A** A different key is used to encrypt each of the bits.
**B** The same key is used to encrypt each of the blocks.
**C** Encryption of plain text is done bit by bit.
**D** Encryption is usually very simple and much faster.

**20** Why **SHOULD** a data custodian enforce an expiration date on key use within a key management system?

**A** It may prevent exhaustion of session keys derived from the master key.
**B** An expiration date should not be enforced within a key management system.
**C** It may prevent enough time to transpire for an exhaustive key search by an attacker.
**D** It will prevent users from choosing weak passwords.

**21** What key exchange system allows secret keys to be shared over unsecured channels?

**A** Bitlocker.
**B** Key Destruction.
**C** Trusted Platform Module.
**D** Diffie-Hellman.

**22** Which of the following is **NOT** a block cipher operating mode?

**A** Cipher Block Chaining (CBC) mode.
**B** Electronic Codebook (ECB) mode.
**C** Cipher Feedback (CFB) mode.
**D** Asymmetric Key Cipher (AKC) mode.

**23** What will impact the probability of a successful brute force attack on an authentication system?

**A** Password entropy.
**B** Number of attempts.
**C** Factors of authentication.
**D** Password length.

**24** What makes a Trusted Platform Module (TPM) immune to malware attacks?

**A** Use of one-time pad for each session.
**B** Encryption key length and complexity.
**C** Hardware device protection.
**D** Use of packet-level firewalls.

**25** Which of the following is the **MOST** suitable algorithm for full disk encryption (FDE)?

**A** SHA256.
**B** PKI.
**C** AES.
**D** PGP.

**26** A Linux administrator creates two users with the same password. On opening the /etc./shadow file the accounts are shown to have different hashed passwords in the following format:

User1: $6$r6ydwb$g9fvdf49sj4m
User2: $6$if2be48$k4jyzw546jcn

What has been added to the password before hashing?

**A** Salt value.
**B** Preimage resistance.
**C** Z notation.
**D** Data inference.

**27** A UK company uses a firewall that provides SSL inspection to investigate unauthorised data egress from their internal systems. Why **SHOULD** consideration be given to who is allowed access to the firewall and any data collected from logs?

**A** An attacker may be able to ARP poison the logs on the firewall.
**B** The decrypted data may contain valid sensitive information from user sessions on the network.
**C** Inspection of the logs may invalidate investigation by police.
**D** In a busy network the logs may grow to an unmanageable size.

**28** What is a keystore used for?

**A** Purchasing SSL certificates online.
**B** Secure storage of cryptographic keys and certificates.
**C** Temporary storage of session keys in AES key expansion.
**D** Cached keys in a hardware security module.

**29** 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.

**30** Which of the following standard covers policy and regulation on the use of cryptographic controls?

**A** ISO 9001.
**B** ISO 27001.
**C** Common criteria.
**D** ISO 17025.

**31** Which statement supports Kerckhoff's **MAJOR** principle?

**A** Kerckhoff's principle is the concept that a cryptographic system should be designed to be secured, even if all of its details, except for the key, are known publicly.
**B** Kerckhoff's principle is the concept that a cryptographic system should be organised to be publicly known even the key can be public.
**C** Kerckhoff's principle is the concept that a cryptographic system should be confidential and secure. None of its details should be known, the key is tightly secured.
**D** Kerckhoff's principle is the concept that a cryptographic system should be designed with easy access and the key should be accessible to those who want it.

**32** GSM security model employs cryptography to implement which of the following functions?

a) Authentication.
b) Confidentiality.
c) Integrity.
d) Non-repudiation.

**A** a and b only.
**B** b and c only.
**C** c and d only.
**D** a and d only.

**33** What key does International Data Encryption Algorithm (IDEA) use?

**A** 128-bit
**B** 164-bit
**C** 64-bit
**D** 32-bit

**34** A company IT department encrypts all employees' laptops with AES256. An employee is travelling to China on business. Why would it be prudent to seek legal advice?

**A** Strong encryption may be subject to an export license agreement.
**B** Licensing for AES does not cover its use outside of the EU.
**C** The user may not be able to contact the server in the UK for a Kerberos token.
**D** The laptop can only be used when it is on the company network.

**35** What does RIPA 2000 stand for?

**A** Regulation of International Powers Act 2000.
**B** Regulation of Investigatory Powers Act 2000.
**C** Regulation of Industry Powers Act 2000.
**D** Regulation of Investigative Powers Act 2000.

**36** What is the role of UK National Cyber Security Centre (NCSC)?

**A** To conduct periodic cyber security health checks for industries and SMEs; and to identify any gap in their cybersecurity readiness.
**B** To provide expert, trusted, and independent guidance for UK based public and private organisations.
**C** To identify those UK based organisations who are vulnerable to cyber-attacks or are not putting efforts to protect themselves from cyber-attacks.
**D** To provide paid cyber security auditing service for UK based organisations and provide specialist advise on securing their resources.

**37** A software developer has decided to use the security of session keys for the protection of their private key that they employ for the decryption of their secure messages. This way they can quickly access the private key for routine use. Who will be responsible if their private key is stolen?

**A** A security solutions (Firewall and IDS) vendor because this incident shows the security products are not working properly.
**B** A system administrator, because the software developers private key may not be stolen without compromising session keys.
**C** A staff security training manager, because software developer may not have appropriate awareness of securing cryptography keys.
**D** The software developer because they used inadequate protection mechanism for their private key.

**38** A citizen of a member country of the Wassenaar Arrangement may travel to any country that has signed the agreement with an encrypted device under a personal use exemption, providing which condition is met?

**A** They do not create, enhance, share, sell or otherwise distribute the encryption technology whilst visiting.
**B** They inform the country they are entering of the intended use of the encryption device.
**C** They inform the authorities of the encryption keys in advance of the visit.
**D** They agree not carry the encryption keys with the encryption device.

**39** 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.

**40** Which of the following is a database of known vulnerabilities in publicly released software packages?

**A** CVE.
**B** ISO.
**C** IDEA.
**D** DSA.

**-End of Paper-**