Making IT
good for society

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

Specimen Paper A

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 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 **two** of the following are certificates used for?

a) Client authentication.
b) WEP encryption.
c) Access control lists.
d) Password hashing.

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

3 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.

4 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.

5 Entropy in a computer system may be used for which one 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.

6 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.

7 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.

8 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.

9 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.

10 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.

11 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.

12 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.

13 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.

14 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.

15 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.

16 Which of the following is an example of 'downgrade attack'?

A MOODLE attack.
B POODLE attack.
C DOODLE attack.
D NODDLE attack.

17 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.

18 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.

19 What is the key length used in the International Data Encryption Algorithm (IDEA)?

A 64-bit.
B 128-bit.
C 256-bit
D 512-bit

20 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.

-End of Paper-