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. The full paper will contain 40 questions with a pass mark for the full paper of 26/40.

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

1) Authentication Headers (AH)
2) Encapsulating Security Payload (ESP)
3) 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) Code signing.
e) Password hashing.

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

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 A VPN.
B An IPSEC Tunnel.
C A Digital Certificate.
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 **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.

7 International Data Encryption Algorithm (IDEA) was developed by Xuejia Lai and whom?

A James Massey.
B Bruce Schneier.
C Carlisle Adams.
D Stafford Tavares.

8 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 1 to 1 correspondence table.
C Plaintext is transformed into a group of random symbols.
D The cipher is changed into a single random symbol.

9 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).

10 Which **two** of the following can be used on a smartphone to **BEST** protect against sensitive data loss if the device is stolen?

a) Tethering.
b) Remote wipe.
c) Email password.
d) GPS tracking.
e) Device encryption.

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

11 A security administrator has been tasked with explaining authentication services to the company's management team. The company runs an active directory infrastructure. Which of the following solutions **BEST** relates to the host authentication protocol within the company's environment?

A Kerberos.
B Least Privilege.
C TACACS+.
D LDAP.

12 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.

13 A way of verifying both the sender of information and the integrity of a message is through the use of which of the following?

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

14 Which of these tools are **MOST LIKELY** to be used during the discovery phase of a penetration test?

A Nessus.
B Wireshark.
C Network Mapper.
D Burp.

15 Which of the following is the **BEST** 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.

16 Which of the following Acts were signed into law in 2000?

A Cyber Security Enhancement Act.
B Online Privacy Protection Act.
C No-Electron Theft Act.
D Electronic Signatures in Global and National Commerce Act.

17 Voice privacy in GSM cellular telephone protocol is provided by which cipher?

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

18 What UK evaluation scheme helps private sector companies develop cryptographic products?

A Federal Information Processing Standards Publication (FIPS).
B Commercial Product Assurance (CPA).
C CESG Assisted Products Service (CAPS).
D Information Technology Security Evaluation and Certification Scheme (ITSEC).

19 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.

20 When a connection is made to a secure HTTPS web page, which of the following actions is performed **first**?

A The username and password are sent for authentication.
B The client establishes its identity to the web server.
C The web page is displayed and then authentication is performed.
D A digital certificate establishes the web site identity to the browser.

-End of Paper-