Professional Course Examination, May 2022

(6th Semester)

BACHELOR OF COMPUTER APPLICATIONS

(Computer Networking—II)

Full Marks : 75

Time : 3 hours

The figures in the margin indicate full marks for the questions

(PART : A—OBJECTIVE)

(*Marks* : 25)

SECTION—I

(*Marks* : 15)

Tick (✓) the correct answer in the brackets provided : 1×10=10

1. The science and art of transforming messages to make them secure and immune to attacks is

   (a) message authentication ( )

   (b) message integrity ( )

   (c) message confidentiality ( )

   (d) cryptography ( )

2. The plaintext is the original message before transformation; the message after transformation is called

   (a) encryption ( )

   (b) decryption ( )

   (c) ciphertext ( )

   (d) cryptography ( )

3. The first ever computer virus, self-replicating virus released in the year 1971 created by Bob Thomas was

(*a*) Brain ( )

(*b*) Creeper ( )

(*c*) Mydoom ( )

(*d*) Slammer ( )

4. An attacker impersonates an authorized device or user to steal data, spread malware, or bypass access control systems is

(*a*) spamming ( )

(*b*) sniffing ( )

(*c*) spoofing ( )

(*d*) hoaxes ( )

5. _____ is a popular session key creator protocol that requires an authentication server and a ticket granting server.

(*a*) KDC ( )

(*b*) Kerberos ( )

(*c*) KDD ( )

(*d*) CA ( )

6. The simplest and the oldest method of entity authentication is

(*a*) private key ( )

(*b*) public key ( )

(*c*) password ( )

(*d*) secret key ( )

7. IPsec defines two protocols _____ and _____.

(*a*) AH,SSL ( )

(*b*) PGP, ESP ( )

(*c*) AH, ESP ( )

(*d*) PGP, SSL ( )

8. Pretty good privacy (PGP) is used in

(*a*) browser security ( )

(*b*) e-mail security ( )

(*c*) FTP security ( )

(*d*) WiFi security ( )

9. A program which is available to check the infected files that are COM or EXE is

(a) Worm Watcher ( )

(b) Antidotes ( )

(c) Malwarebytes ( )

(d) None of the above ( )

10. _____ is an umbrella term used to cover all types of malicious software.

(a) Virus ( )

(b) Worm ( )

(c) Malware ( )

(d) None of the above ( )

Tick (✓) whether the following statements are *True (T) or False (F)* : 1×5=5

11. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are asymmetric key cryptographies.

(T / F)

12. The attackers pretend to be legitimate participant is called man-in-the-middle attack.

(T / F)

13. Asymmetric key cryptographies are blowfish, AES, DES, IDEA, RC5, CAST-128, etc.

(T / F)

14. Modification Detection Code (MDC) is a keyless hash function that can detect any modification in the message.

(T / F)

15. The simplest port scans are ping scans.

(T / F)

SECTION—II

(*Marks* : 10)

Answer the following questions : 2×5=10

1. *(a)* What is Trojan horse?

OR

(b) Explain briefly the two types of sniffing attack.

2. *(a)* In RSA algorithm, if $p = 3$ and $q = 11$, what are the values of n and $\phi(n)$?

OR

(b) What do you understand by Diffie-Hellman cryptosystem?

3. *(a)* Hash function needs to meet three criteria. Justify.

OR

(b) Write two applications of HMAC.

4. *(a)* What is Internet key exchange (IKE)?

OR

(b) What is the basic difference between SSL and TLS?

5. *(a)* What is operating system detection tool?

OR

(b) What do you mean by port scanner?

(PART : B—DESCRIPTIVE)

(*Marks* : 50)

Answer the following questions : 10×5=50

1. *(a)* Differentiate between the folloiwng : 5+5=10

(i) Virus and Worm

(ii) DOS attack and DDOS attack

OR

(b) What is phishing? Explain how to protect against phishing. 5

(c) What is brute-force attack? Explain how to defend against brute-force attack. 5

2. *(a)* Explain the characteristics of RSA algorithm. What are the advantages and disadvantages of RSA algorithm? 10

OR

(b) What do you mean by cryptography? Explain the substitution ciphers and transposition ciphers of symmetric key cryptography with examples. 10

3. *(a)* What do you mean by network security? Explain message confidentiality with symmetric key cryptography and asymmetric key cryptography with suitable diagram. 10

OR

(b) Explain the difference between message authentication and entity authentication. 10

4. *(a)* What is firewall? Explain the difference between packet filter firewall and proxy firewall. 10

OR

(b) Write notes on the following : 5+5=10

(i) Virtual Private Network (VPN)

(ii) Pretty Good Privacy (PGP)

5. *(a)* What is antivirus software? Write the advantages and disadvantages of antivirus. 10

OR

(b) Write notes on the following : 5+5=10

(i) Intrusion detection and prevention system (IDPS)

(ii) Vulnerability scanner

★ ★ ★