Roll No. .... Total Printed Pages -8

F - 1026

M.Sc. (Fourth Semester)
EXAMINATION, May - June, 2022
COMPUTER SCIENCE
Paper Second
(Network Security and Cryptography)

Time : Three Hours] *[Maximum Marks:100*

[Minimum Pass Marks:40

Note: Attempt all section as directed.

(Section - A)
(Objective/Multiple Choice Questions)

(1 mark each)

Note : Attempt all questions.

Choose the correct answer:

1. A digital signature needs a:

   (A) Private Key System

   (B) Shared Key System

   (C) Public Key System

   (D) Secret Key System

2. Following are the examples of message authentication Code.

   (A) HMAC

   (B) CMAC

   (C) SHA- 1

   (D) Both (A) and (B)

3. What is cyber security?

   (A) Cyber security provides security against malware

   (B) Cyber security provides security against cyber- terrorists

   (C) Cyber security protects a system from cyber attacks

   (D) All of the mentioned

4. Which of the following is an objective of network security?

   (A) Confidentiality

   (B) Integrity

   (C) Availability

   (D) All of the above

5. MAC is a -

   (A) One-to-one mapping

   (B) Many-to-one mapping

   (C) Onto mapping

   (D) None of the mentioned

6. Another name for message authentication codes is:

   (A) Cryptographic code break

   (B) Cryptographic code sum

   (C) Cryptographic check sum

   (D) Cryptographic check break

7. In authentication without encryption ________ is not provided.

   (A) Authentication

   (B) Confidentiality

   (C) Integrity

   (D) None of the mentioned

8. Which one of the following modes of operation in DES is used for operating short data?

   (A) Cipher Feedback Mode (CFB)

   (B) Cipher Block Chaining (CBC)

   (C) Electronic Code Book (ECB)

   (D) Output Feedback Modes (OFB)

9. The key used in cryptography

   (A) Public Key

   (B) Private Key

   (C) Secret Key

   (D) All of them

10. How many round keys generated by DES?

   (A) 16 bit

   (B) 32 bit

   (C) 48 bit

   (D) 64 bit

11. In the RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q'?

   (A) p and q should be divisible by $\phi(u)$

   (B) p and q should be co-prime

   (C) p and q should be prime

   (D) p/q should give no remainder

12. Which of the following is/are offered by the Hash functions?

   (A) Authentication

   (B) Non repudiation

   (C) Data Integrity

   (D) All of the above

13. Firewalls are to protect against:

   (A) Virus attacks

   (B) Fire attacks

   (C) Data driven attacks

   (D) Unauthorized attacks

14. Cryptographic hash functions execute faster in software than block ciphers-

    (A) Statement is correct

    (B) Statement is incorrect

    (C) Depends on the hash function

    (D) Depends on the processor

15. What is the value of ipad in the HMAC structure?

    (A) 00111110

    (B) 00110010

    (C) 10110110

    (D) 01110110

16. Data Authentication Algorithm (DDA) is based on:

    (A) DES

    (B) AES

    (C) MD-5

    (D) SHA-1

17. Public Key encryption/decryption is not preferred because

    (A) It is slow

    (B) It is hardware/software intensive

    (C) It has a high computational load

    (D) All of the mentioned

18. Password-based authentication can be divided into two broad categories _______ and _______.

    (A) Fixed, Variable

    (B) Time - Stamped; fixed

    (C) Fixed; one time

    (D) None of the above

19. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bit via _________

    (A) Scaling of the existing bits

    (B) Duplication of the existing bits

    (C) Addition of zeros

    (D) Addition of ones

20. Which one of the following is a key function of firewall?

    (A) Copying

    (B) Moving

    (C) Deleting

    (D) Monitoring

Section - B

(Very Short Answer Type Questions)

(2 marks each)

Note: Attempt all questions.

1. What do you mean by computer security?
2. What is security attack?
3. What do you mean by message authentication?
4. What do you mean by security of hash function?
5. What do you mean by message integrity?
6. What do you mean by MAC?
7. What do you mean by intruders?
8. What is honey pat? Explain in brief.
9. What is firewall and its type?
10. What is wire shark?

Section - C

(Short Answer Type Questions)

(3 marks each)

Note: Attempt all questions.

1. What do you mean by cryptography?
2. What is crypt analysis?

P.T.O.

3. Explain public key cryptography.
4. Explain SHA.
5. Explain HMAC and CMAC.
6. What is digital signature?
7. What are malicious software's?
8. Explain DDoS attack in brief.
9. What do you mean by packet analyzer?
10. Explain in brief Kali Linux.

Section - D

(Long Answer Type Questions)

(6 marks each)

Note: Attempt all questions.

1. Write down the steps involved, in DES algorithm with example.
2. Explain HASH function, its requirement and security.
3. Explain digital signature, purpose, process and its services.
4. Explain virus and its classification.
5. Explain cyber security policy and domain of cyber security policy.