

Total Pages : 8

H-7141

M.Sc. (Semester-IV) Examination, 2022

COMPUTER SCIENCE

(Network Security)

Time Allowed : Three Hours

Maximum Marks : 70

Minimum Passing Marks : 25

Note : Question paper is divided into four sections. Attempt question of all four section as per given direction. Distribution of marks is given in each section.

SECTION - A

Note : Attempt **any ten** questions. Each question carries **1** mark.

1. Fill in the blanks : [10×1=10]

(i) CHAP stands for _____ .

(ii) _____ is the security feature that can control Access resources in the operating system.

H-7141/1000

(1)

[P.T.O.]

- (iii) Message _____ means that the data must arrive at the receiver exactly as sent.
- (iv) A (n) _____ can be used to preserve the integrity of a document or a message.
- (v) _____ means that a sender must not be able to deny sending a message that he sent.
- (vi) A concern of authentication that deals with user rights is known as _____ .

Multiple Choice Question :

- (vii) Which is not an objective of network security?
 - (a) Identification
 - (b) Authentication
 - (c) Access control
 - (d) Lock
- (viii) The Process of verifying the identity of a user :
 - (a) Authentication
 - (b) Identification
 - (c) Validation
 - (d) Verification

- (ix) What is the preferred way of Encryption?
- (a) Pre shared secret key
 - (b) Using key distribution center
 - (c) Public key-encryption
 - (d) Symmetric key
- (x) What is not an Encryption Standard?
- (a) AES
 - (b) TES
 - (c) Triple DES
 - (d) DES
- (xi) Which of the following is not a Stream Cipher?
- (a) Two fish
 - (b) RC_5
 - (c) RC_4
 - (d) TBONE

- (xii) What is a Hash Function?
- (a) It creates a small flexible block of data
 - (b) It creates a small, fixed block of data
 - (c) It creates a encrypted block of data
 - (d) None of the mentioned

SECTION - B

(Very Short Answer Type Questions)

Note : Attempt **any five** questions. Each question carries **2** marks. Maximum word limit is 25-30 words. [5×2=10]

- 2.
- (i) What is Finite Field?
 - (ii) What is the strength of DES Algorithm?
 - (iii) What are Prime numbers?
 - (iv) What PGP? Explain.
 - (v) What is System Security?
 - (vi) What is Security Mechanism?
 - (vii) Define Secure Electronic Transaction?

SECTION - C

(Short Answer Type Questions)

Note : Attempt **any five** questions. Each question carries **4** marks. Maximum word limit is **250** words. [5×4=20]

3. (i) Explain OSI Security Architecture.
- (ii) What is Block Cipher? Explain the Design Principles of Block Cipher.
- (iii) What is Public Key Cryptography? Discuss its Principles.
- (iv) What is Kerberos? Explain with suitable example.
- (v) What is Hacking? Explain various Hacking concepts.
- (vi) What is Virus? Discuss its various types.
- (vii) Write a short note on Euclid's Algorithm.

SECTION - D

(Essay Type Questions)

Note : Attempt **any three** questions. Each question carries **10** marks. Maximum word limit is 500 words. [3×10=30]

4. (i) What is Private Key Cryptography? Explain DES Algorithm with suitable example.
- (ii) Explain RSA Algorithm and Diffie-Hellman Key exchange Algorithm.
- (iii) What is Web Security? Discuss secure socket layer (SSL) and Transport Layer (TL) with suitable example.
- (iv) Explain Firewall and Malicious software with suitable example.

----X----