MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL

Paper Code : CS-801D

CRYPTOGRAPHY & NETWORK SECURITY

Time Allotted : 3 Hours *Full Marks* : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

GROUP – A

(Multiple Choice Type Questions)

1. Choose the correct alternative for the following : $10 \times 1 = 10$

i) Interception is an attack on

a) availability b) confidentiality

c) authenticity d) integrity.

ii) If the recipient of a message has to be satisfied with the identify of the sender, the principle of ..... comes into picture.

a) confidentiality b) authentication

c) integrity d) access control.

iii) The four primary security principles related to message are
   a) confidentiality, authentication, integrity and non-repudiation
   b) confidentiality, access control, non-repudiation and integrity
   c) authentication, authorization, non-repudiation and availability
   d) availability, access control, authorization and authentication.

iv) Conversion of cipher text into plain text is called as
   a) encryption b) decryption
   c) cryptography d) cryptanalyst.

v) Firewall is a specialized form of a
   a) bridge b) disk
   c) printer d) router.

vi) In substitution cipher, which of the following happens ?
   a) Characters are replaced by other characters
   b) Rows are replaced by columns
   c) Columns are replaced by columns
   d) None of these.

vii) There are ..... rounds in DES.
   a) 8 b) 10
   c) 14 d) 16.

viii) DES encrypts blocks of ..... bits.
   a) 32 b) 56
   c) 64 d) 128.

ix) In which attack, there is no modification to message contents ?

a) Passive b) Active

c) Both of these d) None of these.

x) A worm ..... modify a program.

a) does not b) does

c) may d) may or may not.

GROUP – B
(Short Answer Type Questions)

Answer any *three* of the following. 3 × 5 = 15

2. What is the difference between diffusion and confusion ?
3. What are the properties that a digital signature should have ?
4. a) Discuss about the four basic principles related to the security of a message.

   b) What is availability ? 4 + 1
5. Explain the key generation process in DES.
6. What are the problems with symmetric key encryption ?

GROUP – C
(Long Answer Type Questions)

Answer any *three* of the following. 3 × 15 = 45

7. a) What is a worm ? What is the difference between Worm and Virus ?

   b) What are the key principles of security ?

   c) What is DOS (denial-of-service attack) ?

   d) What do you mean by network security ? Explain with a suitable model. (2 + 2) + 4 + 3 + 4

8. a) What do you mean by asymmetric key encryption ? Explain.

   b) What is the difference between symmetric key encryption and asymmetric key encryption ?

   c) Describe CBC mode of encryption process. What is Initialization Vector ? 3 + 4 + 4 + 1 + 3

9. a) Given 2 prime numbers P = 13, Q = 31. Find out N, E, D in RSA encryption process.

   b) Why is the SSL layer positioned between application layer and transpose layer ?

   c) Name the four key steps in the creation of a Digital certificate. How is SHTTP different from SSL ?

   4 + 4 + 4 + 3

10. a) With the help of diagram, briefly explain how public key cryptography works. Explain with a diagram how the addition of a digital signature changes the process of public key cryptography.

    b) Explain the concepts of confusion and diffusion.

    c) Explain the working principle of RC5. 7 + 3 + 5

11. Write short notes on any *three* of the following : 3 × 5

    a) Firewall

    b) Sniffing and spoofing

    c) IDEA

    d) Diffie-Hellman Key-Exchange/Agreement Algorithm

    e) One-Time pad.