Seat No.	

Total No. of Pages : 4

T.Y. B.Tech. (Computer Science and Engineering) (Semester - V) (CBCS) Examination, November - 2023

INFORMATION SECURITY

Sub. Code : 80798

Day and Date : Tuesday, 28 - 11 - 2023 **Total Marks : 70**

Time : 10.30 a.m. to 01.00 p.m.

Instructions : **1)** **All Questions are compulsory.**
2) **Assume suitable data wherever necessary.**
3) **Figures to the right indicate full marks.**

Q1) **MCQs (1 Marks Each)** **[14 × 1 = 14]**

i) _____ Is To Protect Data And Passwords

a) Encryption b) Authentication

c) Authorization d) Non Repudiation

ii) _____ Prevents Either Sender Or Receiver From Denying A Transmitted Message.

a) Non Repudiation b) Data Integrity

c) Active Attack d) Passive Attack

iii) In Playfair cipher technique combining i&j, if PT = MYNAMEISATUL and Keyword = PLAYFAIREXAMPLE, CT=_____

a) XFOLXRMKPVLR b) XFOLIXMKPVLR

c) XFOLXRMKPVRL d) FOLXRMKPVRR

iv) The two keys used for asymmetric encryption are referred to as the _____ and _____

a) public key and private key

b) shared key and secret key

c) public key and shared key

d) secret key and private key

v) In RSA algorithm If two prime numbers are 17 and 11 then value of n will be _____

a) 187 b) 160

c) 178 d) 198

vi) _____ is used on sender side for encryption for getting authentication.

a) Public Key b) Private Key

c) Secret key d) Symmetric key

vii) A variety of approaches has been proposed for the digital signature function. These approaches fall into two categories _____.

a) Direct and arbitrated b) Indirect and arbitrated

c) Direct and indirect d) None of the above

viii) In Kerberos,TGS referred as _____.

a) Ticket granting Server b) Token getting Server

c) Target getting Service d) None of the above

ix) In _____ Mode, the authentication header is inserted immediately after the IP header.

a) Tunnel b) Transport

c) Authentication d) Both a and b

x) IPSec is designed to provide the security at the _____

a) transport layer b) network layer

c) application layer d) session layer

xi) Firewalls operate by _____

a) The pre-purchase phase

b) Isolating intranet from extranet

c) Screening packets to/from the network and provide controllable filtering of network traffic

d) None of the above.

8955 8955 8955

xii) A fundamental tool for intrusion detection is _____.

a) Audit record

b) Password management.

c) Both a & b

d) None of the above

xiii) What is a buffer-overflow attack?

a) Overflowing a port with too many packets

b) Putting more email in an email system than it can hold

c) Overflowing the system

d) Putting more data in a buffer than it can hold

xiv) SQL injection is based on what?

a) Having database admin privileges

b) Creating an SQL statement that is always true

c) Creating an SQL statement that will force access

d) Understanding web programming

Q2) **Solve any 2 of the following (7 Marks Each)** **[2 × 7 = 14]**

a) Explain X.800 Security services?

b) Explain the distribution of public keys using public-key certificates?

c) Give the overview of Kerberos?

Q3) **Solve any 2 of the following (7 Marks Each)** **[2 × 7 = 14]**

a) Explain Play fair cipher with example?

b) Explain RSA Algorithm with example.

c) Explain X.509 certification formats?

Q4) **Solve any 2 of the following (7 Marks Each)** **[2 × 7 = 14]**

a) Explain Applications and Benefits of Ipsec?

b) Explain Different Types of firewalls?

c) Explain Format string attack?

Q5) **Solve any 2 of the following (7 Marks Each)** **[2 × 7 = 14]**

a) Explain Tunnel and Transport mode of IP Security?

b) Explain SSL Record Protocol?

c) Write a short note on Phishing?

8955 8955 8955