Code No: 157CC

R18

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, July/August - 2022
INFORMATION SECURITY
(Information Technology)

Time: 3 Hours **Max.Marks:75**

Answer any five questions
All questions carry equal marks
- - -

1.a) Draw a matrix that shows the relationship between security mechanisms and attacks.
b) List and explain the Strength of DES. [7+8]

2.a) Why do some block cipher modes of operation only use encryption while others use both encryption and decryption? Also, state some differences between Block & Stream ciphers.

b) With the help of a neat diagram, explain the model for Internetwork security. [8+7]

3.a) Consider a Diffie- Hellman key with a common prime q=11 and primitive root $\alpha = 2$, If the user has a public key $Y_a = 9$ what is A's private key X_A.
b) Briefly explain the Public key Cryptography Principles in detail. [5+10]

4. Discuss about Message authentication and Hash Functions. [15]

5.a) List and explain the PGP services and explain how PGP message generation is done with a neat diagram.
b) Mention three variations of digital signatures and briefly state the purpose of each.[8+7]

6.a) Explain the X.509V3 certificate format.
b) In PGP, what is the probability that a user with N public keys will have at least one, duplicate key ID? [8+7]

7.a) Discuss the steps involved in Secure Electronic Transaction.
b) Draw and explain the IP security architecture. [8+7]

8.a) Select any antivirus of your choice and explain it in detail.
b) Where would you place a web server in an organization assuming that you can use a network firewall and why? [8+7]

--ooOoo--