Code No: 157CC

R18

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

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

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

1.a) With the help of a neat diagram, explain the model for network security.
b) Make comparisons between the symmetric cipher model, substitution ciphers, and transposition ciphers. [8+7]

2. For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity respectively. Justify your answers.
a) Financial Organization managing routine administrative information.
b) Organization managing public information on its web server.
c) Law enforcement organizations managing extremely sensitive investigative information. [5+5+5]

3.a) In RSA, Given n=12091 and e=13, encrypt the message "THIS IS TOUGH" using the 00 to 26 encoding scheme. Decrypt the ciphertext to find the original message .
b) Describe the steps in finding the message digest using the SHA-512 algorithm. What is the order of finding two messages having the same message digest? [8+7]

4.a) Explain HMAC.
b) Discuss about authentication requirement. [8+7]

5.a) Assume client C wants to communicate with a server S using Kerberos protocol. How can it be achieved?
b) Why does PGP compress the message? What are the reasons for compressing the signature before encryption? [8+7]

6. Explain the X.509 certificate formats. Why Kerberos is needed? What is one-way authentication? [15]

7. Discuss the IP security architecture and also explain basic combinations of security associations with a neat diagram. [15]

8. Define Firewall. Explain its characteristics, types, services, and limitations. [15]

--ooOoo--