R13

Code No: 126AQ

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech III Year II Semester Examinations, July/August - 2021

INFORMATION SECURITY

(Computer Science and Engineering)

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

Answer any five questions

All questions carry equal marks

\- - -

1.a) Discuss in detail about various types of Security attacks.
b) Give a model for Network Security with neat diagram. [7+8]

2.a) Write short notes on key distribution.
b) In an RSA system, the public key of a given user is e=31, n=3599. What is the private key of this user? [7+8]

3. Explain HMAC algorithm for authentication. [15]

4.a) Write a short note on S/MIME.
b) Give IP Security architecture with neat diagram. [7+8]

5. List the characteristics of a good firewall implementation. How is circuit gateway different from application gateway? [15]

6. With the help of a suitable example, explain the transposition ciphers. [15]

7. Consider a Diffie-Hellman scheme with a common prime q=11, and a primitive root α=2.
a) If user "A" has public key YA=9, what is A's private key XA.
b) If user "B" has public key YB=3, what is shared secret key K. [7+8]

8. Describe the process of X.509 authentication service. [15]

---ooOoo---