Code No: 157BB

R18

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, February/March - 2022
CRYPTOGRAPHY AND NETWORK SECURITY
(Computer Science and Engineering)

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

Answer any Five Questions
All Questions Carry Equal Marks

- - -

1.a) Differentiate between Active attacks and Passive Attacks.
b) Elaborate any four Substitution Technique and list their merits and demerits. [7+8]

2.a) Discuss briefly about categories of Security Services and attacks.
b) Explain the model for network security with neat sketch. [8+7]

3.a) Using RSA algorithm solve n, d if p=11, q=3, e=3. Encrypt "HelloWorld" Message.
b) Give a detailed explanation of key generation and encryption of IDEA algorithm. [6+9]

4. Users A and B use the Diffie Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7, Test the following
a)What is the shared secret key? Also write the algorithm.
b) How man-in-the-middle attack can be performed in Diffie Hellman algorithm. [8+7]

5.a) How the authentication procedures are defined by X.509 certificate. Evaluate the concept of 'Certificate Chain' for verification of Digital Signature on X.509 certificate.
b) Categorize the various servers used in Kerberos. Explain the role of each one. [6+9]

6.a) Discuss briefly about the compression function of Secure Hash Algorithm.
b) Explain the structure of CMAC. Classify the difference between CMAC and HMAC. [8+7]

7.a) What protocols comprise SSL? Distinguish between an SSL connection and an SSL session.
b) Make up the security constraints of IEEE 802.11i Wireless LAN in detail.
c) Compare and contrast the security threats related to mobile devices. [5+5+5]

8.a) Draw the IP security authentication header and identify the functions of each field.
b) What are the principal services provided by S/MIME?
c) How does Pretty Good Privacy provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and elaborate its components. [3+5+7]

---ooOoo---