R17 Regulation *Subject code:* 1P7EA

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

(Autonomous, Accredited by NAAC with 'A' Grade)

B.Tech IV Year I Semester Regular Examinations, February 2021

NETWORK SECURITY & CRYPTOGRAPHY

(Computer Science and Engineering)

Maximum Marks: 70 Date:20.02.2021 Duration: 3 hours

Note: **1.This question paper contains two parts A and B.**
2. Part A is compulsory which carries 20 marks. Answer all questions in Part A.
3. Part B consists of 5 Units. Answer any one full question from each unit.
4. Each question carries 10 marks and may have a, b, c, d as sub questions.

Part-A

All the following questions carry equal marks **(10x2M=20 Marks)**

1 Differentiate attack and threat.
2 Show how to convert the given text "TKREngg" into cipher text using Rail fence technique.
3 Summarize the purpose of S-boxes in DES.
4 Evaluate the formula for encryption and decryption using RSA algorithm.
5 Explain digital signature differs from authentication protocols?
6 Illustrate the design objectives of HMAC.
7 Define S/MIME.
8 Why does PGP generate a signature before applying compression?
9 Describe tunnel mode in IP security.
10 Differentiate host based intrusion detection system and network based intrusion detection system.

Part-B

Answer All the following questions. **(10M X 5=50Marks)**

11 (a) What is Steganography? Briefly examine any three techniques used. (4M)
(b) What is mono-alphabetic cipher? Examine how it differs from Caesar cipher? (6M)

OR

12 With a neat block diagram, explain the network security model and the important parameters associated with it.(10M)

13 Describe the Elliptic curve cryptography with an example. (10M)

OR

14 Explain briefly about Diffie-Hellman key exchange algorithm with its pros and cons.(10M)

15 What is Digital Signature? Explain how it is created at the sender end and retrieved at receiver end. (10M)

OR

16 Explain briefly about the architecture and certification mechanisms in Kerberos and X.509.(10M)

17 Evaluate the different protocols of SSL. (10M)

OR

18 Demonstrate Secure Electronic Transaction with neat diagram. (10M)

19 (a) Discuss about the authentication header of IP. (5M)
(b) Summarize Encapsulating Security Payload of IP. (5M)

OR

20 (a) Discuss the role of intrusion detection system? What are the three benefits that can be provided by the intrusion detection system? (5M)
(b) Discuss the architecture of distributed intrusion detection system with the necessary diagrams. (5M)