Regulation R20 *Subject code:3P7FB*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech VII Semester Supplementary Examinations, April 2024

INFORMATION SECURITY

(IT)

Maximum Marks: 70 Date:30.04.2024 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 which carries 10M.
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 Explain passive attacks.
2 What is interruption?
3 Define linear cryptanalysis.
4 Define approaches are there to attacking the RSA algorithm.
5 Define Hash function.
6 Define Message Authentication Code.
7 List the benefits of IPSec.
8 Explain IP Security.
9 What is Firewall?
10 What are parameters of session state?

Part-B

Answer All the following questions. (10MX 5=50Marks)

11 Explain substitution techniques with suitable examples. [10M]

OR

12 a) Write about steganography? [5M]
b) Explain security mechanisms. [5M]

13 Explain key distribution. [10M]

OR

14 a) Explain how key exchange is done using Diffie-Hellman key exchange.
b) Discuss the "man-in-the-middle" attack. [5+5]

15 Explain HMAC algorithm. [10M]

OR

16 Discuss the requirements of Kerberos. Explain the Kerberos ver-4 message exchanges. [10]

17 Explain the different MIME content types. [10M]

OR

18 Draw the IP security authentication header and explain the functions of each field. [10M]

19 Explain secure electronic transaction. [10M]

OR

20 Discuss about Password Management. [10M]