R18 Regulation *Subject code:2E7FG*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech VII Semester Supplementary Examinations, July 2022

INFORMATION SECURITY

(Information Technology)

Maximum Marks: 70 Date:05.07.2022 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 Write down the different types of attacks?
2 Compare and contrast transposition ciphers and substitution ciphers.
3 Specify the design criteria of block cipher.
4 Write the differences between public key and private key encryption?
5 What is the function of TGS server in Kerberos?
6 Define Message Authentication code.
7 What is IP Security? What are its benefits?
8 List the different encryption and authentication algorithms used for AH and ESP protocols.
9 What do you mean by malicious software?
10 List out different types of firewalls.

Part-B

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

11 A. List and explain different types of Security Attacks. 5m
B. Consider the following: 5m
Plaintext: "KEY"
Secret key: "CRYPTOGRAPHY"
Compute the cipher text from given plain text and key using hill cipher method.

OR

12 A. Explain the transposition techniques. 5m
B. Discuss about Network security model with neat illustration. 5m

13 A. With a neat block diagram explain DES algorithm. 6m
B. In a RSA system, it is given that p = 11, q = 13, e = 7 and M = 5, Find ciphertext C and also M from decryption. 4m

OR

14 Explain AES Algorithm. 10m

15 A. Give the design objectives for HMAC. 4m
B. List the main features of SHA-512 cryptographic hash function. What kind of compression function is used in SHA-512? 6m

OR

16 A. Differentiate between RC5 and blowfish. 5m
B. Give a neat sketch to explain the concept of Secured Hash Algorithm (SHA). 5m

17 A. Explain PGP Message generation and PGP message reception techniques. 5m
B. Explain the different MIME content types. 5m

OR

18 A. What are the applications of IP security? 4m
B. Describe the general structure of IPSEC authentication header. Discuss how anti-reply service is supported. 6m

19 A. Discuss about Intrusion Detection and approaches of Intrusion Detection. 6m
B. What are the various virus counter measures? 4m

OR

20 A. List the characteristics of a good firewall implementation. How is circuit gateway different from application gateway? 5m
B. Explain the steps involved in performing Secure Inter-branch Payment Transactions. 5m