R20 Regulation *Subject code: 3P4HB*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech IV Semester Regular/Supplementary Examinations, September 2023

Information Security

(CSE (DATA SCIENCE))

Maximum Marks: 70 Date:19.09.2023 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 Differentiate passive attack and active attack.
2 Encrypt the plaintext "DOCUMENT" using Caesar cipher with key=3.
3 Mention the advantages of RC4.
4 What are the principle elements of a public key cryptosystem?
5 How is the security of a MAC function expressed?
6 What is Kerberos? Point out its uses.
7 Define SET. What are the features of SET?
8 Define S/MIME.
9 List the benefits of IP Security.
10 What are the three classes of intruders?

Part-B

Answer All the following questions. (5X10M=50Marks)

11 Discuss in detail the OSI Security Architecture highlighting the attacks, mechanisms and services. (10M)

OR

12 Explain the transposition techniques and substitution techniques in detail with suitable examples. (10M)

13 A. Define Block Cipher. Explain Design Principles of block cipher. (5M)
B. What are the differences between stream cipher and block cipher? (5M)

OR

14 A. Explain briefly about RSA and discuss its merit. (5M)
B. Perform using encryption and decryption using RSA algorithm for p=3, q=11, e=7 and for message M=5. (5M)

15 A. What is message authentication? List the authentication requirements. (6M)
B. Compare the principal characteristics of secure hash functions. (4M)

OR

16 A. Give the format for X.509 certificate. How are users' certificates obtained? (5M)
B. Explain the authentication services provided by X.509. (5M)

17 A. Write the steps involved in the simplified form of the SSL / TLS protocol. (5M)
B. Generalize the methodology involved in computing the keys in SSL / TLS protocol. (5M)

OR

18 Evaluate the performance of PGP. Compare it with S/MIME. (10M)

19 A. What is the need for encapsulation of Security Payload? Write and explain different fields of top-level format and substructure of ESP packet. (5M)
B. Discuss about the concept of combining security associations. (5M)

OR

20 A. Explain Password management. (5M)
B. Explain Intrusion detection in detail. (5M)