R18 Regulation

Subject code: 2E6EA

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech VI Semester Regular/Supplementary Examinations, June 2022

INFORMATION SECURITY
(COMPUTER SCIENCE & ENGINEERING)

Maximum Marks: 70 Date:17.06.2022 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 Give various security services.
2 What are the principles of security?
3 Discuss about Blowfish.
4 Specify the applications of the public key cryptosystem.
5 List out message authentication codes.
6 List three approaches to Message Authentication.
7 What are the benefits of IP Security?
8 Differentiate between MIME & S/MIME.
9 List Out Web Security Considerations.
10 Define Transport Layer Security?

Part-B

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

11 A. Discuss in detail about various types of Security attacks with neat diagrams. [5M]
B. Compare and Contrast between Symmetric and Asymmetric key cryptography. [5M]

OR

12 A. Explain the model of network security. [5M]
B. Explain various substitution techniques with suitable examples. [5M]

13 Consider a Diffie-Hellman scheme with a common prime q=11, and a primitive root α=2.
A. If user "A" has public key YA=9, what is A"s private key XA.
B. If user "B" has public key YB=3, what is shared secret key K. [5M+5M]

OR

14 A. With a neat block diagram explain the single round of DES algorithm. [5M]
B. Explain Block Cipher design principles. [5M]

15 A. Give various Hash Functions. Discuss secure hash algorithm with suitable examples. [5M]
B. Explain the approaches for Digital Signatures based on Public Key Encryption. [5M]

OR

16 A. What is HMAC and what are its advantages over MAC? [5M]
B. Write a short note on Kerberos. [5M]

17 A. Explain secure inter branch payment transactions. [5M]
B. Explain IP security architecture. [5M]

OR

18 A. Discuss in detail encapsulating security payload. [5M]
B. Explain about Cross site Scripting Vulnerability. [5M]

19 A. Explain MIME context types. [5M]
B. What are the five principal services provided by PGP? [5M]

OR

20 A. List and briefly define the parameters that define an SSL session state. [5M]
B. Explain in detail about IEEE 802.11i Wireless LAN. [5M]