



R20 Regulation

Subject code: 3P7FB

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech VII Semester Regular Examinations, November 2023

INFORMATION SECURITY (INFORMATION TECHNOLOGY)

Maximum Marks: 70

Date: 12.12.2023 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)

Bloom
Tx

1	Differentiate active and passive attacks.	L2
2	Define steganography.	L1
3	Compare stream cipher with block cipher with example.	L2
4	Mention the advantages of key distribution in cryptography.	L1
5	List the three major classes of message authentication function.	L1
6	Give the main types of biometric authentication methods.	L1
7	Name any four cryptographic keys used in PGP.	L1
8	Mention the two security services provided by IPSec.	L1
9	What are the three classes of intruders?	L1
10	What is virus in information security?	L1

Part-B

Answer All the following questions.

(5X10M=50Marks)

11	a) Consider the following: Plaintext: "KEY" Secret key: "CRYPTOGRAPHY" Compute the cipher text from given plain text and key using hill cipher method. [5] b) Explain the model for network security. [5]	L3 L2
OR		
12	What is the objective of attacking an encryption system? Describe the two approaches to attack a conventional encryption scheme. [10]	L1
13	Explain the scheme for DES encryption. [10]	L1
OR		
14	a) How to determine appropriate Values for e, d, and n in RSA algorithm. [5] b) In an RSA system, the public key of a given user is e=31, n=3599. What is the private key of this user? [5]	L2 L2
15	A. Explain the operation of secure hash algorithm on 512-bit block. [5] B. What are the characteristics needed in a secure hash function? [5]	L2 L2

	OR	
16	Client machine C wants to communicate with server S. Explain how it can be achieved through Kerberos protocol? [10]	L2
17	Explain the operation description of PGP. [10]	L2
	OR	
18	Discuss authentication, header and ESP in detail with their packet format. [10]	L2
19	Explain the steps involved in performing Secure Inter-branch Payment Transactions. [10]	L1
	OR	
20	List the characteristics of a good firewall implementation? How is circuit gateway different from application gateway? [10]	L1