



R18 Regulation

Subject code: 2E6EA

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY
(Autonomous, Accredited by NAAC with 'A' Grade)

B.Tech VI Semester Supplementary Examinations, January 2023
INFORMATION SECURITY

(Computer Science and Engineering)

Maximum Marks: 70

07-01-2023

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.
 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 Define cryptography.
- 2 How would we transform the message "Come Home Tomorrow" using Rail Fence Technique ?
- 3 Define Permutation.
- 4 Given two prime numbers $P=7$ and $Q=17$. Find out N, E , and D in an RSA encryption Process.
- 5 Differentiate session key and master key?
- 6 Discuss digital signatures?
- 7 Enumerate applications of IPSEC?
- 8 Explain parameters identify SA?
- 9 Define PGP?
- 10 Explain S/MIME?

Part-B

Answer All the following questions.

(5X10M=50Marks)

- 11 Consider the following:

Plaintext: "CRYPTOGRAPHY"

Secret key: "KEYS"

Compute the cipher text from given plain text and key using hill cipher method. [10]

OR

- 12 Briefly define the 1. caesar cipher 2. play fair [5+5]
- 13 Compare and contrast DES, 3-DES and AES and explain the principle elements of a public key cryptography. [10]

OR

- 14 Explain various modes of operations about block ciphers. [10]
- 15 Enumerate the different steps of SHA-512 to generate message digest? [10]

OR

- 16 a) List out management functions of PKIX and describe the process in detail? [5]
b) Distinguish between direct and arbitrated digital signature? [5]
- 17 Discuss how IPSEC encompasses three functional areas: [3+3+4]
a) Authentication b) Confidentiality c) Key management
- OR
- 18 Write about Case Studies on Cryptography and security. [10]
- 19 Enumerate all services of PGP and explain with neat sketch. [10]
- OR
- 20 Illustrate S/MIME message? [10]