R22 Regulation *Subject code: 4P7GB*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech VII Semester Regular/Supplementary Examinations, October 2026

INFORMATION SECURITY

(CSE (AI & ML))

Maximum Marks: 60 Date:30.10.2026 Duration: 3 hours

Note: **1.This question paper contains two parts A and B.**
2. Part A is compulsory which carries 10 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 (10X1M=10 Marks)		Marks	CO	BTL
1.a)	Write one limitation of the Caesar cipher.	1M	1	2
b)	Apply a given 2 × 2 key matrix to a plaintext vector.	1M	1	3
c)	What happens when a plaintext block is encrypted using a block cipher?	1M	2	2
d)	Why the final round of AES is different from the other rounds.	1M	2	2
e)	What property makes a hash function computationally difficult to reverse?	1M	3	2
f)	Write the purpose of authentication in Web security.	1M	3	2
g)	How can a man-in-the-middle attack affect web communication?	1M	4	
h)	How SET provides confidentiality for transaction information with the help of dual signature and encryption.	1M	4	2
i)	What is meant by combining Security Associations?	1M	5	2
j)	Differentiate AH and ESP in terms of confidentiality.	1M	5	2

Part-B

Answer All the following questions. (5X10M=50Marks)		Marks	CO	BTL
2	a) Describe the major security mechanisms used to provide network security. b) Compare Caesar, Playfair, and Hill ciphers based on their working principles and security characteristics.	5M 5M	1	3 4
	OR			
3	a) Explain steganography and describe how information can be hidden inside a digital image. b) Encrypt a given plaintext using the Playfair cipher and explain the encryption process.	5M 5M	1	2 3
4	Analyze the security limitations of ECB mode and explain why other modes may be preferred.	10M	2	4
	OR			

5	a) Demonstrate the RSA algorithm using a suitable numerical example. b) Compare RSA and ECC in terms of key size, security, computational requirements, and applications.	5M 5M	2	3 3
6	a) Explain the role of logical functions, message schedule, and round constants in SHA-512. b) Analyze the advantages of using HMAC over simply applying a hash function to a message.	5M 5M	3	2 4
	OR			
7	a) Describe how digital signatures provide authentication, integrity, and non-repudiation. b) Illustrate the concept and architecture of Public Key Infrastructure (PKI).	5M 5M	3	3 2
8	a) Describe the roles of cardholder, merchant, issuer, acquirer, payment gateway, and certificate authority in SET. b) Analyze the security advantages of SET over conventional online payment methods.	5M 5M	4	2 4
	OR			
9	a) Explain how PGP provides confidentiality, authentication, integrity, and compression for e-mail communication. b) Explain how S/MIME ensures confidentiality, integrity, authentication, and non-repudiation.	5M 5M	4	3 3
10	a) Differentiate between IPSec transport mode and tunnel mode. b) Explain how multiple Security Associations can be used to provide different security services.	5M 5M	5	2 2
	OR			
11	a) Explain how an IDS can be used to detect unauthorized access and malicious activities. b) Compare AH and ESP and explain appropriate situations for their use.	5M 5M	5	2 3