PVP 23

Code: 23CS3603, 23IT3602

III B.Tech - II Semester - Regular Examinations – APRIL 2026

CRYPTOGRAPHY & NETWORK SECURITY

(Common for CSE, IT)

Duration: 3 hours Max. Marks: 70

Note: 1. This question paper contains two Parts A and B.
2. Part-A contains 10 short answer questions. Each Question carries 2 Marks.
3. Part-B contains 5 essay questions with an internal choice from each unit. Each Question carries 10 marks.
4. All parts of Question paper must be answered in one place.

BL – Blooms Level CO – Course Outcome

PART – A

		BL	CO
1.a)	Find the difference between active attacks and passive attacks.	L2	CO1
1.b)	Differentiate between security services and mechanisms.	L2	CO1
1.c)	Identify the drawbacks of DES.	L2	CO1
1.d)	Define the Feistel cipher structure.	L1	CO1
1.e)	How asymmetric cryptography is different from symmetric cryptography?	L2	CO1
1.f)	What is a man-in-the-middle attack on Diffie-Hellman?	L1	CO1
1.g)	What is a digital signature?	L1	CO1
1.h)	How does MAC differ from a hash function?	L2	CO1
1.i)	What is the difference between SSL and TLS?	L1	CO1
1.j)	What is ISAKMP? How does it relate to IKE?	L2	CO1

PART – B

			BL	CO	Max. Marks
UNIT-I					
2	a)	Classify and explain all types of cryptographic attacks in detail.	L2	CO1	5 M
	b)	Describe a model for Internetwork security.	L2	CO1	5 M
OR					
3	a)	Discuss the CIA triad (Confidentiality, Integrity, Availability) in detailed.	L2	CO1	5 M
	b)	How Internet Standards (RFCs) can be applied to ensure interoperability in secure communication? Explain.	L2	CO1	5 M
UNIT-II					
4	Describe the DES algorithm in detail with its structure, key schedule, and rounds of operation.		L3	CO4	10 M
OR					
5	a)	Compare Single DES, Double DES, and Triple DES.	L2	CO4	5 M
	b)	Describe the AES algorithm with all four transformations.	L2	CO4	5 M
UNIT-III					
6	a)	Explain public key cryptography principles in detail.	L2	CO4	5 M

	b)	Examine the RSA cryptosystem with complete key generation, encryption, and decryption.	L4	CO4	5 M
OR					
7	a)	Describe the Diffie-Hellman key exchange algorithm.	L2	CO4	5 M
	b)	State the ElGamal encryption algorithm steps briefly.	L2	CO4	5 M
UNIT-IV					
8	a)	Describe digital signature schemes in detail.	L2	CO2	5 M
	b)	What is a Random Oracle Model? State its significance in cryptographic proofs.	L2	CO2	5 M
OR					
9	a)	Analyze the role of SHA-512 in ensuring message integrity.	L4	CO2	5 M
	b)	Explain HMAC construction and its security properties.	L2	CO2	5 M
UNIT-V					
10	a)	Explain the SSL handshake protocol step-by-step with a sequence diagram.	L3	CO3	5 M
	b)	Discuss how PGP ensures confidentiality and authentication.	L2	CO3	5 M
OR					
11	a)	Explain IPSec architecture.	L2	CO3	5 M
	b)	Discuss IPSec two protocols (AH and ESP).	L2	CO3	5 M