PVP 20

Code: 20AM3601, 20DS3601

III B.Tech - II Semester – Regular Examinations - APRIL 2025

CRYPTOGRAPHY AND NETWORK SECURITY

(Common for AIML & DS)

Duration: 3 hours Max. Marks: 70

Note: 1. This paper contains questions from 5 units of Syllabus. Each unit carries 14 marks and have an internal choice of Questions.
2. All parts of Question must be answered in one place.

BL – Blooms Level CO – Course Outcome

			BL	CO	Max. Marks
UNIT-I					
1	Write short notes on				
	a)	Security attacks with appropriate diagrams.	L2	CO1	7 M
	b)	Security services .	L2	CO1	7 M
OR					
2	a)	Write the requirements of Cryptography.	L2	CO1	7 M
	b)	Discuss model for network security.	L2	CO1	7 M
UNIT-II					
3	a)	Illustrate any three substitution ciphers with examples.	L3	CO2	7 M
	b)	Mention the strengths and weakness of DES algorithm.	L2	CO1	7 M
OR					
4	Analyze the general structure of DES algorithm.		L4	CO4	14 M

UNIT-III					
5	a)	Illustrate RSA algorithm for encryption and decryption process with an example.	L3	CO2	7 M
	b)	Explain about Elliptic Curve Cryptography (ECC).	L2	CO1	7 M
OR					
6		Analyze the ElGamal cryptographic system with an example.	L4	CO4	14 M
UNIT-IV					
7	a)	Explain different approaches of NIST Digital Signature Algorithm with relevant diagrams.	L2	CO1	7 M
	b)	Summarize the properties of Hash Function.	L2	CO1	7 M
OR					
8	a)	Identify the security services provided by digital signature.	L2	CO1	7 M
	b)	Analyze the process involved in message digest generation and processing of single block in SHA-512.	L4	CO4	7 M
UNIT-V					
9	a)	Explain briefly about PGP.	L2	CO1	7 M
	b)	What is S/MIME? Explain its operational description in email security.	L2	CO1	7 M
OR					

10	a)	Analyze the Internet Mail Architecture and its components.	L4	CO4	7 M
	b)	Explain about IP security overview.	L2	CO1	7 M