BONAM VENKATA CHALAMAYYA INSTITUTE OF TECHNOLOGY & SCIENCE
(AUTONOMOUS)
II – MCA III - Semester Regular Examinations (BR23), December 2024
Cryptography and Network Security (MCA)

Time: 3 hours   Max. Marks: 70

Answer any Five Questions One Question for One UNIT
ALL the Question Carry Equal Marks

	UNIT-I	Marks	CO	BL
1.a)	Describe CryptographicAttack? What are the different types of attacks?	7M	CO1	BL1
b)	Describe the algebraic structure?	7M	CO1	BL2
	OR			
2.a)	Discuss about substitution Cyphers.	7M	CO1	BL2
b)	Explain about DES Algorithm with an example	7M	CO1	BL2

	UNIT-II	Marks	CO	BL
3.a)	Illustrate the Fermat's Little Theorem	7M	CO2	BL4
b)	Discuss about Chinese Remainder theorem	7M	CO2	BL2
	OR			
4.a)	Define asymmetric? Explain about asymmetric Encryption with example?	7M	CO2	BL1
b)	Discuss the RSA algorithm for asymmetric cryptography	7M	CO2	BL2

	UNIT-III	Marks	CO	BL
5.a)	Explain about message Integrity	7M	CO3	BL2
b)	Determine A cryptographic Hash function	7M	CO3	BL3
	OR			
6.a)	Explain about SHA-512 in detail	7M	CO3	BL2
b)	Illustrate briefly about the Elgamal Digital signature schemes	7M	CO3	BL4

	UNIT-IV	Marks	CO	BL
7.a)	Explain How Symmetric key distribution	7M	CO4	BL2
b)	Describe the public key distribution	7M	CO4	BL4
	OR			
8.a)	Explain about X.509 certificates.	7M	CO4	BL2
b)	Describe the user authentication using symmetric Encryption	7M	CO4	BL2

	UNIT-V	Marks	CO	BL
9.a)	Explain the internet mail architecture	7M	CO5	BL2
b)	Illustrate about PGP perform trust processing	7M	CO5	BL4
	OR			
10.a)	Illustrate the S/MIME	7M	CO5	BL4
b)	Describe the IP security Policy.	7M	CO5	BL2

****

Bonam Venkata Chalamayya Institute of Technology & Science (Autonomous)

Department of Computer Applications

Course: CRYPTOGRAPHY AND NETWORK SECURITY (C214)   Year / Semester : II / III

Branch: MCA

Faculty :R.N.L.BHAVANI   **Academic Year: 2024-2025**

Course Outcomes

Following this course, students will be able to

C214.1: Describe various attacks on the network and understanding the need for security
Apply various classical encryption techniques on messages and analyze various
security services and mechanisms. [Understand]

C214.2: Compare and contrast symmetric and asymmetric Key Cryptography systems.
[Analysis]

C214.3: Describe the cryptographic hash functions, message authentication codes and various key
management and distribution techniques. [Understand]

C214.4: Explain different protocols like SSL, PLS, HTTPS, SSH and various wireless network
standards.[Analysis]

C214.5: Analyze how PGP and S/MIME is used to protect messages transmitted through E-mail and
explains IPSEC. [Evaluation]

Faculty

HOD