Course Code	Course Name	Course Type	Cd	L	T	P	Marks		
							Sessional	Final Exam	Total
COM-403	Foundations of Cryptography	PCC	4	3	1	0	50	100	150

Course Outcomes:

At the end of the course the student will be able to	
CO1	Explain the principles of security, types of attacks, and importance of encryption techniques.
CO2	Demonstrate understanding and application of symmetric and asymmetric key cryptography.
CO3	Apply public key cryptography and message authentication methods.
CO4	Describe the concepts, methods, and classifications of data compression techniques.
CO5	Implement and compare different entropy and source encoding methods in data compression.

Detailed Syllabus

Section-A

Unit 1: Mathematical Foundations: Integer Arithmetic, Set of Integers, Binary Operations, Integer Division, Divisibility, Linear Diophantine Equations, **modular arithmetic:** Modulo Operator, Set of Residues: Zn, Congruence, Operations in Zn, Inverses, Addition and Multiplication Tables, Different Sets for Addition and Multiplication.**(8 Hrs.)**

Unit 2: Introduction to simple Encryption techniques: Secret-key encryption, public-key, block and stream ciphers, hybrid encryption, Message authentication codes, Nonrepudiation, certificates. **(8 Hrs.)**

Unit 3: Classical Encryption Techniques: The Shift Cipher, Substitution Cipher, Affine Cipher, Hill Cipher, Permutation Cipher, Stream Cipher, Cryptanalysis: Affine Cipher, Substitution Cipher, Vigenere Cipher, Hill Cipher Stream Cipher, One-Time Pad. **(8 Hrs.)**

Section-B

Unit 4: Modern Encryption Techniques: Piling-up Lemma, Linear Approximations of S-boxes, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Hash Functions and data integrity, SHA-512, Message and Message Digest encryption. **(9 Hrs.)**

Unit 5: Public Key Encryption Techniques: ElGamal Cryptosystem, Shanks' Algorithm, Diffie-Hellman Problems, RSA algorithm, Signing and Encrypting, Multivariate encryption technique. **(7 Hrs.)**

Text Books

S. No.	Name of the Books	Author	Publisher	Edition (Pub. Yr.)
1	Cryptography and Network security Principles and practice	William Stallings	Prentice Hall	7th (2017)
2	Cryptography and Network Security	Behrouz A. Forouzan	McGraw Hill Education	2nd (2020)

Reference Books

S. No.	Name of the Books	Author	Publisher	Edition (Pub. Yr.)
1	Cryptography Theory and Practice	Douglas R. Stinson Maura B. Paterson	CRC Press	6th (2019)