CRYPTOGRAPHY & NETWORK SECURITY

Course Code	**23CS3603**	**Year**	III	**Semester**	II
Course Category	**Core**	**Branch**	**CSE**	**Course Type**	Theory
Credits	3	**L – T – P**	3-0-0	**Prerequisites**	Computer Networks, Operating Systems
Continuous Evaluation:	30	**Semester End Evaluation:**	70	**Total Marks:**	100

Course Outcomes		
Upon successful completion of the course, the student will be able to:		
CO1	Understand core cryptography and network security principles for building secure systems.	L2
CO2	Apply hashing, digital signatures, and key management techniques to ensure message integrity, authentication, and secure key distribution.	L3
CO3	Apply network security protocols and system security mechanisms to secure communication and networks.	L3
CO4	Analyze symmetric and asymmetric encryption algorithms for data confidentiality, secure key exchange, and authentication.	L4

Syllabus

Unit No.	CONTENTS	Mapped CO
I	**Basic Principles:** Security Goals, Cryptographic Attacks, Services and Mechanisms, A model for Internetwork security, Internet Standards and RFCs.	**CO1**
II	**Symmetric Encryption:** Introduction to Modern Symmetric Key Ciphers-modern block ciphers, Data Encryption Standard- DES structure, DES analysis, Security of DES, Multiple DES, Advanced Encryption Standard-transformations, key expansions, Analysis of AES.	**CO1, CO4**
III	**Asymmetric Encryption**: Public key cryptography principles, Asymmetric Key Cryptography- RSA crypto system, Rabin cryptosystem, Elgamal Crypto system, Diffie-Hellmen key exchange algorithms	**CO1, CO4**
IV	**Data Integrity, Digital Signature Schemes & Key Management:** Message Integrity and Message Authentication-message integrity, Random Oracle model, Message authentication, Cryptographic Hash Functions-SHA-512, Digital Signature- process, services, attacks, Key Management-symmetric key distribution, Kerberos.	**CO1, CO2**

V	**Network Security-I:** Security at application layer: PGP and S/MIME, Security at the Transport Layer: SSL and TLS, **Network Security-II:** Security at the Network Layer: IPSec-two modes, two security protocols, IKE, ISAKMP.	**CO1, CO3**

Learning Resources
Text Books
1. Cryptography and Network Security, 3rd Edition Behrouz A Forouzan, Deb deep Mukhopadhyay, McGraw Hill,2015 2. Cryptography and Network Security,4th Edition, William Stallings, (6e) Pearson,2006 Everyday Cryptography, 1st Edition, Keith M.Martin, Oxford,2016
Reference Books
1. Network Security and Cryptography, 1st Edition, Bernard Meneges, Cengage Learning,2018
E-Resources & other digital material
1. Cryptography and Network Security, NPTEL 2. Cryptography, Coursera 3. Cryptography and Hashing Fundamentals, Udemy