Cryptography and Information Security

Course Code	20CS4501B	**Year**	III	**Semester**	I
Course Category	PEC	**Branch**	CSE	**Course Type**	Theory
Credits	3	**L-T-P**	3-0-0	**Prerequisites**	-
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 the Basic concepts of security over the network.	**L2**
CO2	Apply various Key Management Techniques for secure key sharing.	**L3**
CO3	Analyze encryption algorithms and security protocols for their strengths and weaknesses	**L4**

Contribution of Course Outcomes towards achievement of Program Outcomes & Strength of correlations (3:Substantial, 2: Moderate, 1:Slight)

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	3													
CO2						1	1							2
CO3						1	1		1	1				3

Syllabus		Mapped CO
Unit No.	**Contents**	
I	**Security Concepts:** The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security. **Classical Encryption Techniques:** Substitution Techniques and Transposition Techniques.	**CO1**
II	**Block Ciphers and the Data Encryption Standard:** Traditional Block Cipher Structure, The Data Encryption Standard, Advanced Encryption Standard, Block Cipher operation.	**CO1, CO3**
III	**Public key cryptography:** Principles, RSA, Diffie-Hellman key exchange algorithm. **Cryptographic Hash Functions:** Secure Hash Algorithm (SHA-512), MACs Based on Hash Functions: HMAC, MACs Based on Block Ciphers: DAA and CMAC.	**CO1, CO3**
IV	**Key Management and Distribution:** Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys, X.509 Certificates. Public-Key Infrastructure, Kerberos	**CO1, CO2**
V	**Email Security:** S/MIME, Pretty Good Privacy. **IP Security**: IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange.	**CO1, CO3**

Learning Resources
Text Books
1. William Stallings. Cryptography and Network Security – Principles and Practice, Seventh edition, Pearson Education, 2017.
References
1. Cryptography and Network Security, Forouzan and Mukhopadhyay, Third edition, 2015, Mc Graw Hill. 2. Cryptography and Network Security, Atul Kahate, Third edition,Mc Graw Hill,2013.
e-Resources & other digital material
1. http://nptel.ac.in/courses/106105031/lecture, Dr. Debdeep Mukhopadhyay, IIT Kharagpur 2. https://www.coursera.org/learn/information-security-data 3. https://www.coursera.org/learn/number-theory-cryptography