CRYPTOGRAPHY AND NETWORK SECURITY

Course Code	1**9IT3701**	**Year**	IV	**Semester**	I
Course Category	PC	**Branch**	IT	**Course Type**	Theory
Credits	3	**L-T-P**	3-0-0	**Prerequisites**	Number Theory and Cryptography
Continuous Internal Evaluation :	30	**Semester End Evaluation:**	70	**Total Marks:**	100

Course Outcomes		
Upon Successful completion of course, the student will be able to		**Blooms Taxonomy Level**
CO1	Understand basic concepts of security over the network	L2
CO2	Illustrate the issues in Key Management and Distribution	L2
CO3	Demonstrate the fundamentals of Transport-Level Security and Email security	L2
CO4	Apply various cryptographic concepts in developing security related applications	L3

Contribution of Course Outcomes towards achievement of Program Outcomes & Strength of correlations (H:High, M: Medium, L:Low)

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	3												2	2
CO2	3												2	2
CO3	3												2	2
CO4			3										2	2

Syllabus		
Unit No	**Contents**	**Mapped CO**
I	**Security Concepts**: Introduction, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security **Symmetric Key Ciphers**: Block Ciphers , DES , Block Cipher Principles, Stream Ciphers, RC4	CO1
II	**Cryptographic Hash Functions**: Message Authentication , Secure Hash Algorithm(SHA-512) **Message Authentication Codes**: Message Authentication Requirements, MAC's Based on Block Ciphers: DAA and CMAC **Digital Signatures**: Digital Signatures, Elgamal Digital Signature, Schnorr Digital Signature, NIST Digital Signature Algorithm	CO1, CO4
III	**Key Management and Distribution**: Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys.	CO1, CO2, CO4
IV	**Transport-Level Security**: Web Security Considerations, Secure Sockets Layer, Transport Layer Security, HTTPS, Secure Shell(SSH)	CO1, CO3, CO4
V	**Email Security**: Pretty Good Privacy, S/MIME **IP Security**: IP Security Overview, IP Security Policy	CO1, CO3, CO4

Learning Resources

Text Books

1. William Stallings. Cryptography and Network Security – Principles and Practice, 7/e. Pearson Education, 2014.

Reference Books

1. Atul Kahate, Cryptography and Network Security, 3/e. Mc Graw Hill, 2013.
2. C K Shyamala, N Harini, Dr T R Padmanabhan. Cryptography and Network Security, 1/e. Wiley India, 2011.
3. Forouzan and Mukhopadhyay. Cryptography and Network Security, 3/e. Mc Graw Hill, 2015.
4. Mark Stamp. Information Security, Principles, and Practice. Wiley India, 2011.
5. WM. Arthur Conklin and Greg White. Principles of Computer Security. TMH, 2016.
6. Neal Krawetz . Introduction to Network Security. CENGAGE Learning, 2007.

e-Resources & Other Digital Material

1. http://nptel.ac.in/courses/106105031/lecture by Dr. Debdeep Mukhopadhyay, IIT Kharagpur
2. http://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf