Cryptography and Information Security

Course Code	19CS4601B	**Year**	III	**Semester**	II
Course Category	Program Electi - II	**Branch**	CSE	**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 the course, the student will be able to		
CO1	Understand the need of security over the network	L2
CO2	Apply various cryptographic techniques for providing authentication.	L3
CO3	Apply various Key Management Techniques for secure key sharing.	L3
CO4	Apply various security protocols for real-time applications.	L3

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							1						
CO2	3												2	
CO3	3								3	3			1	
CO4	3					1	1							1

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 Cipher Principles, Blow fish, IDEA, Stream Ciphers, RC4	**CO1,CO2**
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, Schnorr Digital Signature, NIST Digital Signature Algorithm	**CO1,CO2**
III	**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.	**CO1,CO3**
IV	**Transport-Level Security:** Web Security Considerations, Secure Sockets Layer, Transport Layer Security, HTTPS, Secure Shell(SSH)	**CO1,CO4**
V	**Email Security:** Pretty Good Privacy, S/MIME **IP Security**: IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange	**CO1,CO4**

Learning Resources
Text Books
1. William Stallings. Cryptography and Network Security – Principles and Practice, Seventh edition, 2017, Pearson Education.
References
1. Cryptography and Network Security, Atul Kahate, Third edition, 2013, Mc Graw Hill. 2. Cryptography and Network Security, C K Shyamala, N Harini, Dr T R Padmanabhan. First edition, 2011, Wiley India. 3. Cryptography and Network Security, Forouzan and Mukhopadhyay, Third edition, 2015, Mc Graw Hill. 4. Information Security, Principles, and Practice, Mark Stamp, 2011, Wiley India. 5. Principles of Computer Security, WM. Arthur Conklin and Greg White, 2016, TMH. 6. Introduction to Network Security, Neal Krawetz, 2007, CENGAGE Learning.
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