INFORMATION SECURITY

(Professional Elective – I)

Course Code	20IT4501A	**Year**	III	**Semester**	I
Course Category	PE - 1	**Branch**	IT	**Course Type**	Theory
Credits	3	**L-T-P**	3-0-0	**Prerequisites**	Number Theory Computer Networks
Continuous Internal Evaluation :	30	**Semester End Evaluation:**	70	**Total Marks:**	100

Course Outcomes		**Blooms Taxonomy Level**
Upon Successful completion of course, the student will be able to		
CO1	Understand the need of security, cryptographic mechanism and risks in computer systems and network	L2
CO2	Apply appropriate encryption principles and security mechanism in network transmission.	L3
CO3	Apply network security concepts in various real world scenarios.	L3
CO4	Analyze about system security mechanisms.	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												3	
CO2	3					3							3	
CO3	3					3							3	
CO4		3				3							3	

Syllabus		
Unit No	**Contents**	**Mapped CO**
I	Computer Security Concepts, Security Attacks, Security Services Mechanisms, A model for network security, Standards.	CO1
II	Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Random and Pseudorandom Numbers, Stream Ciphers and RC4 , Cipher Block Modes of Operation, Approaches to Message Authentication, Secure Hash Functions, Message Authentication Codes, Public-Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures.	CO1 CO2
III	Key Distribution and User Authentication, Symmetric Key Distribution Using Symmetric Encryption, Kerberos, Key Distribution Using Asymmetric Encryption, X.509 Certificates, Public-Key Infrastructure, Federated Identity Management Transport-Level Security, Web Security Considerations, Secure Socket Layer and Transport Layer Security, Transport Layer Security HTTPS, Secure Shell (SSH)	CO1 CO2 CO3
IV	Electronic Mail Security, Pretty Good Privacy, S/MIME , Domain Keys Identified Mail , IP Security Overview , IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange	CO1 CO3
V	Intruders, Intrusion Detection, Password Management, Types of Malicious Software, Viruses, Virus Countermeasures, Worms, Distributed Denial of Service Attacks, The Need for Firewalls, Firewall Characteristics, Types of Firewalls	CO1 CO4

Learning Resources
Text Books
1. Network Security Essentials Applications and Standards, William Stallings, Pearson Education. 4th Edition, 2011
References
1. Security in Computing, Fourth Edition, by Charles P. Pfleeger, Pearson Education 2. Cryptography And Network Security Principles And Practice, Fourth or Fifth Edition, William Stallings, Pearson 3. Modern Cryptography: Theory and Practice, by Wenbo Mao, Prentice Hall. 4. Principles of Information Security, Whitman, Thomson.5. Introduction to Cryptography, Buchmann, Springer.
E- Resources and other Digital Material 1. https://nptel.ac.in/courses/106106129