Year: M. Tech. II (Semester – III)

Subject Name: Public Key Infrastructure and Trust Management **Subject Code:** MTCO14302
Type of course: Professional Elective - V
Prerequisite: Exposure to Information Security and applications, Mathematical Foundation for Computer Science

List of Courses where this course will be prerequisite: --

Rationale: This course introduces the concepts of public key crypto-system and infrastructure, digital certificates and its importance in the public key infrastructure, user authentication mechanisms and integration of PKI with real-time applications.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
3	0	2	4	60	25	15	30	20	150

CA1: Continuous Assessment (assignments/projects/open book tests/closed book tests. CA2: Sincerity in attending classes/class tests/ timely submissions of assignments/self-learning attitude/solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work/Quality of work submitted/Active participation in lab sessions/viva on practical skills learned in course

Contents:

Unit No	Contents	Total Hrs
1	Introduction to Public Key Cryptography and Public-Key Cryptosystem Cryptography basics, RSA, Diffie-Helman, Key-Exchange, Elgamal Cryptographic System, Elliptic Curve Cryptography, Public Key Cryptography Standards	8
2	PKI Architecture: Digital Signature, RSA-PSS Digital Signature Algorithm, Digital Certificate, Certificate Management, CA Functions, PKI components, Types of PKI Architecture - Single CA Architecture, Enterprise PKI Architecture, Hierarchical PKI Architecture, Mesh PKI Architecture, Hybrid PKI Architecture, concepts of PKI Trust	8

3	Key Management and Distribution: Introduction, Symmetric key distribution using asymmetric encryption, public key distribution, A Simple Protocol using KDC, Otway-Rees Protocol	6
4	User Authentication Mechanisms: Remote User-Authentication Principles, Remote User-Authentication using Asymmetric Encryption, Kerberos, Federated Identity Management, Personal Identity Verification	8
5	Network and Internet Security : Network Access Control and Cloud Security, Transport Level Security, Wireless Network Security, Electronic mail Security, IP Security	12
6	Integrating A Pki With Applications: Implementing a PKI solution to support a selected environment, Advanced topics	3

Reference Books:

Sr.No	Title of book /article	Author(s)	Publisher and details like ISBN	Year of publication	Publication Edition
1	Cryptography and Network Security - Principles and Practice	William Stalings	Pearson		7ed
2	Cryptography and Network Security	Atul Kahate	McGraw Hill		4ed
3	Cryptography and Network Security	B Forouzan, D Mukhopadhyay	McGraw Hill		3ed,

Course Outcomes (CO):

Sr.No.	CO statement	Marks % weightage
1	Differentiate between public key cryptography and infrastructure.	20%
2	Utilize the necessary components of a certificate policy and practices for management and distribution of public keys.	30%

3	Demonstrate Remote User-Authentication mechanism using Asymmetric Encryption	30%
4	Detect and solve network security issues in real-time applications	20%

List of Experiments:

Sr. No.	Practical
1	Demonstrate public key cryptography using RSA algorithm for single-character.
2	Demonstrate public key cryptography using RSA algorithm for a block of characters.
3	Implement Diffie-Hellman Key exchange algorithm.
4	Implement a program that accepts a message from the user. The program must also generate and verify a digital signature for the given message.
5	Check password strength (Weak, Medium, Strong, Very Strong). Setting optional requirements by required length, with at least 1 special character, numbers and letters in uppercase or lowercase.