BCSE330L	PUBLIC KEY INFRASTRUCTURE AND TRUST MANAGEMENT	L	T	P	C
		3	0	0	3
Pre-requisite		**Syllabus version**			
		1.0			

Course Objectives:

1. To provide the knowledge on Public Key Cryptography techniques and Public Key infrastructure.
2. To study about the Digital Certificates and the security challenges.
3. To understand the various trust models and the trust management systems.

Course Outcome:

After completion of this course, the student shall be able to:

1. Analyze and design Public Key cryptographic algorithms.
2. Evaluate the components of PKI and design & integrate PKI services
3. Design the Digital Certificates with PKI considerations
4. Identify the access control mechanism and provide solution for the security challenges
5. Analyze and select suitable trust model and manage with operational considerations

Module:1	**Public Key Cryptography Basics**	**5 hours**

Public Key Cryptography: Secret key, Public key, public/private key pair, Services of public key cryptography - RABIN Cryptosystem - ElGamal Cryptosystem - Message Integrity and Authentication: Random Oracle model, message authentication, Cryptographic hash functions.

Module:2	**Public Key Infrastructure**	**7 hours**

Components and architecture of fully functional Public key infrastructure(PKI): Certification authority, Certificate repository, Certificate revocation, Key backup and recovery, Automatic key update, Key history management, Cross-certification, Support for non-repudiation, Time stamping, Client software, Core PKI Services, PKI-Enabled Services, PKI interoperability, deployment and assessment PKI data structures - PKI architectures: Single CA, Hierarchical PKI, Mesh PKI, Trust Lists, Bridge Certification Authority (CA), Registration Authority (RA), Simple PKI (SPKI), PKI application : Smart card integration with PKI's.

Module:3	**Digital Certificates**	**7 hours**

Introduction to Digital Certificate - Certificate Structure and Semantics - Alternative Certificate Formats - Certificate Policies - Object Identifiers - Policy Authorities - Certification Authority - Key/Certificate Life Cycle Management - Certificate Revocation - Representing certificates in terms of S-Expressions - Certificate Chain.

Module:4	**Access Control Mechanisms and Security Challenges**	**7 hours**

Access Control Mechanisms: Discretionary Access Control (DAC) – Mandatory Access Control (MAC) – Role Based Access Control (RBAC) - Issues : Revocation- Anonymity-Privacy issues - Entity Authentication - Passwords and Challenge Response - zero-knowledge and bio-metrics - Key management - security key distribution – Kerberos - Symmetric Key agreement - Public Key Distribution and Hi-jacking - Issues of revocation - Anonymity and Privacy.

Module:5	**Trust Models**	**7 hours**
Distributed Trust Architecture - Mesh Configuration - Hub-and-Spoke Configuration – Four-Corner Trust Model - Web Model - User-Centric Trust - Cross-Certification - Entity Naming - Certificate Path Processing - Path Construction - Path Validation - Trust Anchor Considerations - Multiple Key Pairs - Key Pair Uses - Relationship between Key Pairs and Certificates.		
Module:6	**Trust Management Systems**	**5 hours**
Social network based Trust Management System- Reputation based Trust Management System (DMRep, EigenRep, P2Prep) - Framework for Trust Establishment - Risks Impact on E-Commerce and E- Business: Information Risk and Technology Business Risk.		
Module:7	**Operational Considerations**	**5 hours**
Client-Side Software - Off-line Operations - Physical Security - Hardware Components - User Key Compromise - Disaster Preparation and Recovery - Relying Party Notification – Preparation – Recovery - Electronic Signature Legislation and Considerations.		
Module:8	**Contemporary Issues**	**2 hours**
	Total Lecture hours:	**45 hours**

Text Book(s)	
1.	John R. Vacca, Public Key Infrastructure: Building Trusted Applications and Web Services, 2019, 1st edition. Auerbach Publications, US.
2.	Carlisle Adams, Steve Lloyd, Understanding PKI: Concepts, Standards, and Deployment Considerations, 2011, 2nd Edition, Addison-Wesley, US.
Reference Books	
1.	Buchmann J, Karatsiolis E, Wiesmaier A, Karatsiolis E., Introduction to public key infrastructures, 2013, Berlin: Springer.

Mode of Evaluation: CAT / written assignment / Quiz / FAT			
Recommended by Board of Studies	04-03-2022		
Approved by Academic Council	No. 65	Date	17-03-2022