CSE2703	Introduction to Cryptography	L	T	P	C
Version 1.0	Date of Approval:	3	0	0	3
Pre-requisites/Exposure	--				
Co-requisites					

Course Objectives

1. Understand OSI security architecture and classical encryption techniques.
2. Acquire fundamental knowledge on the concepts of finite fields and number theory.
3. Understand various block cipher and stream cipher models.
4. Describe the principles of public key cryptosystems, hash functions and digital signature

Course Outcomes

On completion of this course, the students will be able to
CO1: Should be able to learn about basic security concepts
CO2: Should be able to write code for relevant cryptographic algorithms.
CO3: Should be able to asymmetric cryptographic algorithms
CO4: Should be able to learn symmetric key algorithms.
CO5: Should be able to determine basic user authentication concepts

Catalog Description

The objective of this course is to provide the students with an introduction to the internals of Security in network. This course also includes the basic concepts of security, networking, and further leading to core concepts of cryptography. The classification of cryptography into symmetric and asymmetric along with the algorithms like RSA, advanced encryption standards are included. Class activities include reviewing security aspects, cryptographic techniques.

Course Content

Unit 1. Introduction: 6 Lecture Hours

Introduction to security, Need for security, Principles of Security, Introduction to computer networks, OSI Model, TCP/IP model, Attacks, Classification of attacks, Concepts of Viruses, Worms, Trojan Horses

Unit 2. Basics of Modern Cryptography 7 Lecture Hours

Classical Cryptography ,Plain text and Cipher Text, Substitution techniques, Caesar Cipher, Mono-alphabetic Cipher, Polyalphabetic Substitution, Play fair, Hill Cipher,

Transposition techniques, Encryption and Decryption, Symmetric and Asymmetric Key Cryptography

Unit 3. Symmetric Key Cryptography 8 Lecture Hours

Introduction to public key cryptography, Cryptanalysis, Cipher Structure, Encryption Algorithms, Data Encryption Standard (DES), Handshaking protocols, Modes of Operation, Symmetric Block Ciphers, Cipher Block Chaining (CBC)

Unit4 Asymmetric Key Cryptography 7 Lecture Hours

Brief history of Asymmetric Key Cryptography, Overview of Asymmetric Key Cryptography, RSA algorithm, Symmetric and Asymmetric key cryptography together, Diffie-Hellman Key Exchange

Unit 5: User Authentication: 8 Lecture Hours

Network Security, Firewalls and Virtual Private Networks: Brief Introduction to TCP/IP, Firewalls, IP Security, Virtual Private Networks (VPN), Intrusion, Authentication basics, Passwords, Authentication Tokens, Certificate-based Authentication, Biometric Authentication, Web Security

Text / Reference books :

1. D. R. Stinson. Cryptography: Theory and Practice. CRC Press

2. William Stallings, Network Security Essentials-Applications & Standards, Pearson.

3. Charlie Kaufman, Radia Perlman, Mike Speciner, Nework Security Private Communication in a Public World, Second Edition, 2004,Pearson.

4. Matt Bishop, Computer Security, Art and Science, Pearson

5. Bruce Schneier, Applied Cryptography, Pearson

Modes of Evaluation: Quiz/Assignment/ Seminar/Written Examination
Examination Scheme:

Components	MSE I	MSE II	Quiz/Assignment/Seminars etc	ESE
Weightage (%)	10	10	20	60

Relationship between the Course Outcomes (COs) and Program Outcomes (POs)

Mapping between COs and POs

	Course Outcomes (COs)	Mapped Programme Outcomes
CO1	Should be able to learn about basic security concepts	**PO1**
CO2	Should be able to write code for relevant cryptographic algorithms.	**PO1,PO2**
CO3	Should be able to asymmetric cryptographic algorithms	**PO2,PO3**
CO4	Should be able to learn symmetric key algorithms.	**PO1,PO3**
CO5	Should be able to determine basic user authentication concepts	**PO1,PO3**

		Engineering Knowledge	Problem analysis	Design/development of solutions	Conduct investigations of complex problems	Modern tool usage	The engineer and society	Environment and sustainability	Ethics	Individual or team work	Communication	Project management and finance	Life-long Learning
Course Code:	Course Title	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO12
CSE2703	Introduction to Cryptography	1,2, 4	2, 3	3,4, 5									

1=weakly mapped

2= moderately mapped

3=strongly mapped