SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
CE702T(iii)	Cryptography & Network Security	4	-	-	4	30	70	100

Course Objectives	Course Outcomes
This course is intended ● 1. To develop the student's ability to understand the concept of security goals in the various applications. ● 2. To provide the students with some fundamental cryptographic mathematics used in various symmetric and asymmetric key cryptography. ● 3. To develop the student's ability to analyze the cryptographic algorithms. ● 4. To familiarize the student with the need of security management in computer network related applications.	**Students will be able to** ● 1. Acquire knowledge about security goals, background of cryptographic mathematics and identification of its application. ● 2. Understand, analyze and implement the symmetric key algorithm. ● 3. Acquire knowledge about the background of mathematics of asymmetric ● 4. Analyze the concept of message integrity and the algorithms for checking the integrity of data. ● 5. To understand various network security techniques to protect against the threats in the networks.

Unit I	**[9 Hrs]**
Introduction, Terminology, Attacks, Security goals, Model for network security, Substitution & Transposition techniques, Mathematics for cryptography: Modular arithmetic, Euclidean, Extended Euclidean algorithm.	
Unit II	**[9 Hrs]**
Symmetric Key Cryptography: Introduction, Block Cipher principles, Data Encryption Standard: DES, Triple DES, Attacks on DES, Blowfish, Advanced Encryption Standard (AES), Stream Cipher principles: RC4.	
Unit III	**[9 Hrs]**
Asymmetric Key Cryptography: Euler's Totient function, Fermat's & Euler's Theorem, Chinese Remainder Theorem (CRT), RSA, Elliptic Curve Cryptography (ECC), Digital Signature.	
Unit IV	**[9 Hrs]**
Key Management & Authentication: Introduction, Kerberos, Key Management Protocol: Diffie Hellman Key Exchange Algorithm, Digital Certificate: X.509 certificate, Hash Function: Introduction to SHA-1, SHA-256, MD5.	
Unit V	**[9 Hrs]**
Network Security: Firewalls & its principal design, Electronic Payment types: E-cash, chip card transaction & attacks, IDS, Software vulnerability: Phishing attack, Buffer overflow, Types of Intruders & its detection: virus, worms and trojan & its countermeasures.	

Text Books

S.N	Title	Authors	Edition	Publisher
1	Cryptography and Network Security: Principles and Standards	William Stallings	7th Edition	Prentice Hall India
2	Network Security and Cryptography	Bernard Menezes	1st Edition	Cengage Learning

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Network Security, The Complete Reference	Robert Bragge, Mark Rhodes, Heithstraggberg	1st Edition	McGraw-Hill
2	Cryptography and Network Security	Behrouz A. Forouzan	2nd Edition	McGraw-Hill
3	Applied Cryptography	Bruce Schneier	2nd Edition	John Wiley

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
CE702P(iii)	Cryptography & Network Security Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended • To understand basics of Cryptography and Network Security. • To be able to secure a message over insecure channel by various means. • To learn about how to maintain the Confidentiality, Integrity and Availability of a data.	**Students will be able to** • Interpret security fundamentals and implement the cipher techniques. • Analyze and implement the key management and key distribution techniques. • Demonstrate the techniques to ensure data security and integrity.

Expt. No.	Title of the experiment
1	Implement Substitution Cipher techniques
2	Implement Transposition Cipher techniques
3	Implement Euclid's algorithm and Extended Euclid Algorithm
4	Implement the following regarding modern block cipher components: 1. WAP a program that splits an n-bit word into two words, each of n/2 bits. 2. WAP that combines two n/2 bits words into n-bit word. 3. WAP that swaps the left and right halves of an n- bit word. 4. WAP that circular- shifts an n-bit word k bits to the left or right based on the first parameter passed to the routine. 5. WAP to show the mapping for straight n x m P-box. 6. WAP to find the order of the permutation group and key size for n x m transposition and substitution block cipher method.
5	To explore Triple DES using virtual lab.
6	To perform round key transformation & Key Expansion process for AES-128 version symmetric key cryptography algorithm.
7	To understand the implementation of Asymmetric key cryptographic algorithm using RSA algorithm & Euler's Totient Function.
8	Implement Mathematical theorems related to Asymmetric Key Cryptography: Fermat's Little Theorem and Chinese Remainder Theorem.
9	Implementation of Cryptographic Hash function using SHA-1 hashing algorithm.
10	To understand the creation of session key using Diffie Hellman Key Exchange algorithm.
11	Mini Project: Students need to create a virtual lab for any of the cryptographic algorithm as per the syllabus.

Text Books

S. No	Title	Authors	Edition	Publisher
1	Cryptography and Network Security: Principles and Standards	William Stallings	7th Edition	Prentice Hall India
2	Network Security and Cryptography	Bernard Menezes	1st Edition	Cengage Learning