Subject Name: Cryptography and Network Security

Subject Code: CE 601

Teaching Scheme (Credits and Hours)

Teaching scheme				Total Credit	Evaluation Scheme					
L	T	P	Total		Theory		Mid Sem Exam	CIA	Pract.	Total
Hrs	Hrs	Hrs	Hrs		Hrs	Marks	Marks	Marks	Marks	Marks
03	00	02	05	4	3	70	30	20	30	150

Learning Objectives:

This course will provide students with a practical and theoretical knowledge of cryptography and network security. By the end of the course, students should be able to:

- Understand the fundamental principles of access control models and techniques, authentication and secure system design.
- Have a strong understanding of different cryptographic protocols and techniques and be able to use them.
- Apply methods for authentication, access control, intrusion detection and prevention.
- Indentify and mitigate software security vulnerabilities in existing systems.

Outline of the Course:

Sr. No	Title of the Unit	Minimum Hours
1	Introduction	2
2	Classical Cryptography	3
3	Block Ciphers (DES, AES)	5
4	Math Background	8
5	Public-Key Cryptography	8
7	Hash and MAC Algorithms, Digital Signatures	5
8	Key Management	4
9	Web Security: IPSec, SSL and TLS	5
10	Email Security : S/MIME and PGP	5

Total hours (Theory): 45

Total hours (Lab): 30

Total hours: 75

Detailed Syllabus

Sr. No	Topic	Lecture Hours	Weightage(%)
1	Introduction : Introduction to Cryptography, Security Threats, Vulnerability, Active and Passive attacks, Security services and mechanism, Conventional Encryption Model, CIA model	2	5
2	Math Background : Modular Arithmatic, Euclidean and Extended Euclidean algorithm, Prime numbers, Fermat and Euler's Theorem	3	20
3	Classical Cryptography : Dimensions of Cryptography, Classical Cryptographic Techniques	5	5
4	Block Ciphers (DES, AES) : Feistal Cipher Structure, Simplifies DES, DES, Double and Triple DES, Block Cipher design Principles, AES, Modes of Operations	8	10
5	Public-Key Cryptography : Principles Of Public-Key Cryptography, RSA Algorithm, Key Management, Diffie-Hellman Key Exchange, Elgamal Algorithm, Elliptic Curve Cryptography	8	20
6	Hash and MAC Algorithms : Authentication Requirement, Functions, Message Authentication Code, Hash Functions, Security Of Hash Functions And Macs, MD5 Message Digest Algorithm, Secure Hash Algorithm, Digital Signatures	5	10
7	Key Management : Key Distribution Techniques, Kerberos	4	10
8	Security in Networks : Threats in networks, Network Security Controls – Architecture, Encryption, Content Integrity, Strong Authentication, Access Controls, Wireless Security, Honeypots, Traffic flow security, Firewalls – Design and Types of Firewalls, Personal Firewalls, IDS, Email Security – PGP, S/MIME	10	20
	Total	**45**	**100**

Instructional Method and Pedagogy:

- At the start of course, the course delivery pattern, prerequisite of the subject will be discussed.
- Lectures will be conducted with the aid of multi-media projector, black board, OHP etc.
- Attendance is compulsory in lecture and laboratory which carries 10 marks in overall evaluation.
- One internal exam will be conducted as a part of internal theory evaluation.
- Assignments based on the course content will be given to the students for each unit and will be evaluated at regular interval evaluation.
- Surprise tests/Quizzes/Seminar/tutorial will be conducted having a share of five marks in the overall internal evaluation.
- The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures.
- Experiments shall be performed in the laboratory related to course contents.

Learning Outcome:

At the end of the course the students will be able to do following:

1. Understand cryptography and network security concepts and application
2. Apply security principles to system design
3. Identify and investigate network security threat
4. Analyze and design network security protocols
5. Conduct research in network security

Reference Books:

1. Cryptography And Network Security Principles And Practice Fourth Edition, William Stallings, Pearson Education
2. Modern Cryptography: Theory and Practice, by Wenbo Mao, Prentice Hall PTR
3. Network Security Essentials: Applications and Standards, by William Stallings. Prentice Hall
4. Cryptography: Theory and Practice by Douglas R. Stinson, CRC press.

List of experiments:

Sr. No.	Name of Practical
01	W.A.P. to implement Ceaser Cipher
02	W.A.P. to implement Affine Cipher with equation c=3x+12
03	W.A.P. to implement Playfair Cipher with key ldrp
04	W.A.P. to implement polyalphabetic Cipher
05	W.A.P. to implement AutoKey Cipher
06	W.A.P. to implement Hill Cipher. (Use any matrix but find the inverse yourself)
07	W.A.P. to implement Rail fence technique
08	W.A.P. to implement Simple Columner Transposition technique
09	W.A.P. to implement Advanced Columner Transposition technique
10	W.A.P. to implement Euclidean Algorithm
11	W.A.P. to implement Advanced Euclidean Algorithm
12	W.A.P. to implement Simple RSA Algorithm with small numbers