IV Year-I Semester		T	P	C
		4	0	3
CRYPTOGRAPHY AND NETWORK SECURITY (RT41051)				

Prerequisite Course:

Computer Networks

Course Description and Objectives:

The main objective of this course is to teach students to understand and how to address various software security problems in a secure and controlled environment. During this course the students will gain knowledge (both theoretical and practical) in various kinds of software security problems, and techniques that could be used to protect the software from security threats. The students will also learn to understand the "modus operandi" of adversaries; which could be used for increasing software dependability.

Course Outcomes:

Upon completion of the course, the student will be able to achieve the following outcomes.

Cos	Course Outcomes	POs
1	Analyze software security problems and protection techniques on both an abstract and a more technically advanced level.	9
2	Explain the basic concepts of cryptography and network security.	9
3	Summarize differences between stream Ciphers and block ciphers & can outline Data Encryption Standard.	11
4	Explain number theory; describe Cryptographic hash functions and digital Signatures.	8
5	Describe about transport layer and email security.	7
6	Describe IP security and intrusion detection systems.	5

Syllabus:

UNIT I: Classical Encryption Techniques

Objectives: *The Objectives of this unit is to present an overview of cryptography, understand the threats & attacks, understand ethical hacking.*

Introduction: Security attacks, services & mechanisms, Symmetric Cipher Model, Substitution Techniques, Transportation Techniques, Cyber threats and their defense (Phishing Defensive measures, web based attacks, SQL injection & Defense techniques)(TEXT BOOK 2), Buffer overflow & format string vulnerabilities, TCP session hijacking(ARP attacks, route table modification) UDP hijacking (man-in-the-middle attacks)(TEXT BOOK 3).

UNIT II: Block Ciphers & Symmetric Key Cryptography

Objectives: *The Objectives of this unit is to understand the difference between stream ciphers block ciphers, present an overview of the Feistel Cipher and explain the encryption and decryption, present an overview of DES, Triple DES, Blowfish, IDEA.*

Traditional Block Cipher Structure, DES, Block Cipher Design Principles, AES-Structure, Transformation functions, Key Expansion, Blowfish, CAST-128, IDEA, Block Cipher Modes of Operations

UNIT III: Number Theory & Asymmetric Key Cryptography

Objectives: *Presents the basic principles of public key cryptography, Distinct uses of public key cryptosystems*

Number Theory: Prime and Relatively Prime Numbers, Modular Arithmetic, Fermat's and Euler's Theorems, The Chinese Remainder theorem, Discrete logarithms.

Public Key Cryptography: Principles, public key cryptography algorithms, RSA Algorithms, Diffie Hellman Key Exchange, Elgamal encryption & decryption, Elliptic Curve Cryptography.

UNIT IV: Cryptographic Hash Functions & Digital Signatures

Objectives: *Present overview of the basic structure of cryptographic functions, Message Authentication Codes, Understand the operation of SHA-512, HMAC, Digital Signature*

Application of Cryptographic hash Functions, Requirements & Security, Secure Hash Algorithm, Message Authentication Functions, Requirements & Security, HMAC & CMAC. Digital Signatures, NIST Digital Signature Algorithm. Key management & distribution.

UNIT V: User Authentication, Transport Layer Security & Email Security

Objectives: *Present an overview of techniques for remote user authentication, Kerberos, Summarize Web Security threats and Web traffic security approaches, overview of SSL & TLS. Present an overview of electronic mail security.*

User Authentication: Remote user authentication principles, Kerberos

Transport Level Security: Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Shell (SSH)

Electronic Mail Security: Pretty Good Privacy (PGP) and S/MIME.

UNIT VI: IP Security & Intrusion Detection Systems

Objectives: *Provide an overview of IP Security, concept of security association, Intrusion Detection Techniques*

IP Security: IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

Intrusion detection: Overview, Approaches for IDS/IPS, Signature based IDS, Host based IDS/IPS. (TEXT BOOK (2)

TEXT BOOKS:

1. Cryptography & Network Security: Principles and Practices, William Stallings, PEA, Sixth edition.
2. Introduction to Computer Networks & Cyber Security, Chwan Hwa Wu, J.David Irwin, CRC press
3. Hack Proofing your Network, Russell, Kaminsky, Forest Puppy, Wiley Dreamtech.

REFERENCE BOOKS:

1. Everyday Cryptography, Fundamental Principles & Applications, Keith Martin, Oxford
2. Network Security & Cryptography, Bernard Menezes, Cengage,2010