IV Year II Semester

Code: 17CS802

L	**T**	**P**	**C**
3	**1**	**0**	**3**

CRYTOGRAPHY AND NETWORK SECURITY

Course objectives:

1. In this course the following principles and practice of cryptography and network security are covered
2. Classical systems, symmetric block ciphers (DES, AES, other contemporary symmetric ciphers)
3. Public-key cryptography (RSA, discrete logarithms)
4. Algorithms for factoring and discrete logarithms, cryptographic protocols, hash functions, authentication, key management, key exchange, signature schemes
5. Email and web security, viruses, firewalls, digital right management, and other topics.

UNIT I : Classical Encryption Techniques Objectives: The Objectives of this unit is to present an overview of the main concepts 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)

Course Outcomes:

- To be familiarity with information security awareness and a clear understanding of its importance.
- To master fundamentals of secret and public cryptography
- To master protocols for security services
- To be familiar with network security threats and countermeasures
- To be familiar with network security designs using available secure solutions (such as PGP, SSL, IPSec, etc)

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