NETWORK SECURITY AND CRYPTOGRAPHY

(Common to SE, CSE & Cyber Security)

Course Code: 13IT2111	**L**	**P**	**C**
	4	**0**	**3**

Pre requisites: Discrete Mathematical Structures.

Course Outcomes:

At the end of the course, a student will be able to

CO 1: Discuss Security Architecture and techniques.
CO 2: Illustrate Symmetric and Public-Key Cryptographic Algorithms
CO 3: Use number theory in Authentication Techniques.
CO 4: Examine authentication algorithms and their applications.
CO 5: Discuss IP security and threats.

UNIT-I

Introduction: Attacks, Services and Mechanisms, Security attacks, Security services, A Model for Internetwork security. Classical Techniques: Conventional Encryption model, Steganography, Classical Encryption Techniques.

Modern Techniques: Simplified DES, Block Cipher Principles, Data Encryption standard, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of operations. Algorithms: Triple DES, International Data Encryption algorithm, Blowfish, RC5, CAST-128, RC2, Characteristics of Advanced Symmetric block ciphers.

UNIT-II

Conventional Encryption: Placement of Encryption function, Traffic confidentiality, Key distribution, Random Number Generation. Public Key Cryptography: Principles, RSA Algorithm, Key Management, Diffie-Hellman Key exchange, Elliptic Curve Cryptography.

UNIT-III

Number theory: Prime and Relatively prime numbers, Modular arithmetic, Fermat’s and Euler’s theorems, Testing for primality, Euclid’s Algorithm, the Chinese remainder theorem, Discrete logarithms. Message authentication and Hash functions: Authentication requirements and functions, Message Authentication, Hash functions, Security of Hash function and MACs.

UNIT-IV

Hash and Mac Algorithms: MD File, Message digest Algorithm, Secure Hash Algorithm, RIPEMD-160, HMAC. Digital signatures and Authentication protocols: Digital signatures, Authentication Protocols, Digital signature standards.

Authentication Applications: Kerberos, X.509 directory Authentication service. Electronic Mail Security: Pretty Good Privacy, S/MIME.

UNIT-V

IP Security: Overview, Architecture, Authentication, Encapsulating Security Payload Combining security Associations, Key Management. Web Security: Web Security requirements, Secure sockets layer and Transport layer security, Secure Electronic Transaction.

Intruders, Viruses and Worms: Intruders, Viruses and Related threats. Fire Walls: Fire wall Design Principles, Trusted systems.

Text books:

1. William Stallings, *Cryptography and Network Security Principles and Practices*, 5th Edition, PHI/Pearson, 2011.
2. William Stallings, *Network Security Essentials Applications and Standards*, 4thEdition, Pearson Education, 2011.

References:

1. Eric Maiwald, *Fundamentals of Network Security*, 1 Edition, Dreamtech press,2008.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, *Network Security Private Communication in a Public World*, 2nd Edition, Pearson/PHI, 2009.
3. Whitman, *Principles of Information Security*, 3rd Edition, Thomson, 2008.
4. Robert Bragg, Mark Rhodes, *Network Security The complete Reference*, 4th Edition, TMH, 2009.
5. Buchmann, *Introduction to Cryptography*, 2nd Edition, Springer, 2009.

Web references:

http://nptel.iitm.ac.in/courses/106105031