NETWORK SECURITY AND CRYPTOGRAPHY

COURSE CODE: 20CT1115

L	T	P	C
3	0	0	3

Pre-requisites: COMPUTER NETWORKS

Course Outcomes: At the end of the Course the student shall be able to

CO 1: Apply various symmetric key cipher methods. (L3)

CO 2: Apply various public key crypto systems.(L3)

CO 3: Explain Hash and MAC algorithms.(L2)

CO 4: Explain key distribution and authentication protocols.(L2)

CO 5: Explain IP security issues and protection mechanisms from malicious software.(L2)

UNIT-I (11 Lectures)

COMPUTER AND NETWORK SECURITY CONCEPTS: Computer Security concepts, the OSI Security architecture, Security attacks, Security services, Security mechanisms, a model for Network Security

CLASSICAL ENCRYPTION TECHNIQUES: Symmetric cipher model, Substitution techniques, Transposition techniques, Steganography

BLOCK CIPHERS AND THE DATA ENCRYPTION STANDARD: Traditional block cipher structure, the Data Encryption Standard, the strength of DES, Block cipher design principles

BLOCK CIPHER OPERATION: Multiple encryption and triple DES, Electronic codebook, Cipher block chaining mode

RANDOM BIT GENERATION AND STREAM CIPHERS: Principles of pseudorandom number generation, pseudorandom number generators, Stream ciphers, RC4

Learning Outcomes: At the end of the module student will be able to:

1. Summarize basic security concepts.(L2)
2. Apply various symmetric encryption techniques (L3)
3. Apply stream cipher concept. (L3)

UNIT-II (11 Lectures)

INTRODUCTION TO NUMBER THEORY: Divisibility and the division algorithm, the Euclidean algorithm, modular arithmetic, prime numbers, Fermat's and Euler's theorems, testing for primality, the Chinese remainder theorem, Discrete logarithms.

PUBLIC-KEY CRYPTOGRAPHY AND RSA: Principles of Public-key cryptosystems, the RSA algorithm

OTHER PUBLIC-KEY CRYPTOSYSTEMS: Diffie-Hellman key exchange, Elgamal cryptographic system, Elliptic curve arithmetic, Elliptic curve cryptography.

Learning Outcomes: At the end of the module student will be able to:

1. Apply number theory concepts. (L3)
2. Compare and contrast various asymmetric encryption techniques. (L2)
3. Explain key exchange algorithms. (L2)

UNIT-III (8 Lectures)

CRYPTOGRAPHIC HASH FUNCTIONS: Applications of cryptographic hash functions, hash functions based on cipher block chaining, Secure Hash Algorithm (SHA)

MESSAGE AUTHENTICATION CODES: Message authentication requirements, Message authentication functions, MACs based on Hash functions: HMAC

DIGITAL SIGNATURES: Digital signatures, Elgamal digital signature scheme, Schnorr digital signature scheme, NIST digital signature algorithm, Elliptic curve digital signature algorithm

Learning Outcomes: At the end of the module student will be able to:

1. Describe cryptographic hash functions. (L2)
2. Describe message authentication codes. (L2)
3. Explain digital signature concepts. (L2)

UNIT-IV (10 Lectures)

KEY MANAGEMENT AND DISTRIBUTION: Symmetric key distribution using symmetric encryption, Symmetric key distribution using asymmetric encryption, distribution of public keys, X.509 certificates, Public-Key Infrastructure

USER AUTHENTICATION: Remote user-authentication principles, Remote user-authentication using Symmetric encryption, Kerberos

TRANSPORT-LEVEL SECURITY: Web security considerations, Transport Layer Security, HTTPS

WIRELESS NETWORK SECURITY: Wireless security, Mobile device security

Learning Outcomes: At the end of the module student will be able to:

1. Describe key distribution concepts. (L2)
2. Describe user authentication protocols. (L2)
3. Explain transport layer security. (L2)

UNIT-V (10 Lectures)

CLOUD SECURITY: Cloud computing, Cloud security risks and countermeasures

ELECTRONIC MAIL SECURITY: Pretty Good Privacy, S/MIME.

IP SECURITY: IP security overview, IP security policy, encapsulating security payload, combining security associations.

MALICIOUS SOFTWARE: Types of Malicious software (Malware), Virus propagation and infected content, Vulnerability exploitation using worms. (Chapter 10, Text Book -2)

INTRUDERS: Intruders, Intrusion detection.(Chapter 11, Text Book -2)

FIREWALLS: The need for firewalls, firewall characteristics and access policy, types of firewalls, firewall configurations. (Chapter 12, Text Book -2)

Learning Outcomes: At the end of the module student will be able to:

1. Explain cloud and E-mail security concepts. (L2)
2. Describe intrusion detection and vulnerability exploits. (L2)
3. Describe the need and usage of firewalls. (L2)

TEXT BOOKS:

1. William Stallings, "*Cryptography and Network Security- Principles and Practice*",7th Edition, Pearson Education, 2017.
2. William Stallings, "*Network Security Essentials-Applications and Standards*", 6th Edition, Pearson Education, 2018

REFERENCE BOOKS:

1. Behrouz A. Forouzan and Debdeep Mukhopadhyay, "*Cryptography and Network Security*", 3rd Edition, Mcgraw Hill Education, 2015
2. Daras, Nicholas J., Rassias, Michael Th, "*Computation, Cryptography, and Network Security*",1st Editon, Springer, 2015
3. T R Padmanabhan, C K Shyamala, N Harini, "*Cryptography and Security*", 1st Edition, WILEY, 2011
4. James S. Kraft and Lawrence C. Washington, "*An Introduction to Number Theory with Cryptography*", 1st Edition, CRC Press, 2013

WEB REFERENCES:

1. https://swayam.gov.in/nd1_noc20_cs21/preview
2. https://www.nist.gov/topics/cybersecurity