S.N	Course Code	Course Title	Course Type	Credit	Week
5	23ONMCH605	**Network Security and Cryptography**	Prog. Core	4	12
PRE-REQUISITE		--			

a. Course Objectives

1. To introduce various encryption and authentication techniques for network security
2. To obtain knowledge on standard algorithms used to provide confidentiality, authenticity, and Integrity
3. To secure a message over the insecure channel by various means.

b. Course Outcomes

CO1	Identify standard algorithms to provide confidentiality, authentication and integrity of the data over the networks
CO2	Understand Security services and policies to provide a secure network.
CO3	Classify Cryptographic techniques for network security.
CO4	Implement cryptographic techniques for message passing to secured network
CO5	Evaluate the performance of the network using Firewall and packet filtering techniques

c. Syllabus

Module-1	**Introduction to Network Security**
Introduction to Security	Introduction to Security: Need for security, Security approaches, Policies of security, Types of attacks, Services: confidentiality, integrity, availability.
Encryption Techniques	Encryption Techniques: Plaintext, Cipher text, Substitution & Transposition techniques, Encryption & Decryption, Cryptographic attacks, Key range & Size. Symmetric & Asymmetric Key Cryptography: Algorithm types &Modes, DES, IDEA, Differential & Linear Cryptanalysis, Symmetric & Asymmetric key together.
Authentication	Authentication basics, Passwords, Authentication tokens, Certificate based & Biometric authentication.
SELF STUDY TOPIC	Knapsack algorithm
Module-2	**Authentication**
Cryptography	Cryptography: Secure inter branch payment transactions, Conventional Encryption and Message Confidentiality, Conventional Encryption Principles, Conventional Encryption Algorithms
Key Distribution & Management	Key Distribution & Management: KDC, Kerberos and certificate authorities
Public Key Cryptography	Public Key Cryptography and Message Authentication: Approaches to Message Authentication, handshake mechanism, Hash function, SHA-1, MD4, MD5, Public-Key Cryptography Principles, RSA, Digital Signatures.
SELF STUDY TOPIC	Location of Encryption Devices
Module -3	**Firewalls and Web Security**
Firewalls	Packet filters, Application-level gateways, Encrypted tunnels, Cookies, Web security problems
Email Security	Distribution lists, Establishing keys, Privacy, source authentication, message integrity, non-repudiation, proof of submission, proof of delivery, message flow confidentiality, anonymity, Pretty Good Privacy (PGP).
SELF STUDY TOPIC	Viruses and malware

d. Self-study topics for Advance learners:Knapsack algorithm, Location of Encryption Devices, Viruses and malware

e. Textbooks / Reference Books

1. Douglas Stinson, "Cryptography Theory and Practice", 2 nd Edition, Chapman & Hall/CRC.

2. B. A. Forouzan, "Cryptography & Network Security", Tata Mc Graw Hill.

3. W. Stallings, "Cryptography and Network Security", Pearson Education.

4. Kaufman, c., Perlman, R., and Speciner, M., Network Security, Private Communication in a public world, 2nd ed., Prentice Hall PTR., 2002.

5. Cryptography and Network Security; McGraw Hill; Behrouz A Forouzan.

6. Information Security Intelligence Cryptographic Principles and App. Calabrese Thomson

f. Assessment Pattern

Internal Assessment Weightage (%)	External Assessment Weightage (%)	Total Weightage(%)
30	**70**	**100**