

L	P	C
3	-	3

20MC207 CRYPTOGRAPHY AND NETWORK SECURITY

Objective of the Course:

This course focuses on the modern concepts of network security using various cryptographic algorithms and underlying network security applications. It also focuses on security implementation in practical applications such as e-mail functioning, web security and secure electronic transactions protocol.

Course Outcomes:

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

COs	Course Outcomes	POs
1	Understand and apply classical encryption techniques, block and stream cipher encryption techniques.	1
2	Analyze the data encryption stands with real time examples	2
3	Analyze protocols used in web security and Transport layer security	2
4	Simulate symmetric and asymmetric cipher and their use in networks	5

Skills:

- Implement symmetric and asymmetric encryption techniques.
- Hands-on security tools like GnuPG, KF Sensor and Net Strumbler.
- Identifying the appropriate firewall, password management and anti-virus models for specific applications.

Activities:

- Implementation of cipher techniques such as (DES, AES and RSA etc...)
- Analyzing the various web security protocols (SSL, TSL and SET etc...)
- Performing case study with either of the open source tools for network security and analysis.

Syllabus

UNIT – 1

9 Hours

NETWORK SECURITY ESSENTIALS: Security trends, Security attacks, Security services, Security mechanisms, A model for network security model, Classical encryption techniques – Symmetric cipher model – Substitution techniques – Caesar cipher- Mono-alphabetic cipher- Playfair cipher- Vigenere cipher; Transposition Techniques –Rail fence cipher, Transposition cipher.

UNIT – 2

9 Hours

BLOCK CIPHERS AND DATA ENCRYPTION STANDARD: Block cipher principles – Data Encryption Standard, Strength of DES, Differential and Linear Cryptanalysis, Block cipher design principles; Advanced Encryption Standard – Evaluation criteria of AES, AES Cipher; More on Symmetric Ciphers – Multiple encryption and Triple DES.

UNIT – 3**9 Hours**

PUBLIC-KEY ENCRYPTION AND HASH FUNCTIONS: Principles of Public-Key cryptosystems – RSA Algorithm, Key Management; Message Authentication and Hash Functions – Authentication Requirements, Authentication Functions, Message Authentication, Hash Functions.

UNIT – 4**9 Hours**

SECURITY APPLICATIONS: Kerberos, X.509 Authentication Service, Public-Key Infrastructure - Public key distribution, Pretty Good Privacy.

UNIT – 5**9 Hours**

WEB AND SYSTEM SECURITY: Secure Electronic Transaction; Intrusion detection, Password management, Malicious software, Firewalls, Trusted Systems.

LIST OF EXPERIMENTS:

1. Implement the following **SUBSTITUTION TECHNIQUES**
 - a) Caesar Cipher
 - b) Playfair Cipher
2. Implement the following **TRANSPOSITION TECHNIQUES**
 - a) Hill Cipher
 - b) Vigenere Cipher
 - c) Rail fence – row & Column Transformation
3. Implement the DES algorithm
4. Implement the RSA algorithm
5. Implement the Diffie-Hellman algorithm
6. Implement the Signature Scheme - Digital Signature Standard
7. Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG)

Text Books:

1. William Stallings, “Cryptography and Network security”, 4th Edition, Pearson Education, 2010.
2. William Stallings “Network Security Essentials Applications and Standards”, 2nd Edition, Pearson Education, 2009.

Reference Books:

1. Eric Malwald, “Fundamentals of Network Security”, 4th Edition, Pearson Education, 2010.
2. Charlie Kaufman, “Radis Perlman and Mike Speciner, Network Security-Private Communication in a Public World”, 1st Edition, Pearson Education, 2009.
3. Buchmann, “Introduction to Cryptography”, 2nd Edition, Pearson Education, 2009.