Cryptography

Course Title: Cryptography
Course No: CSC327
Nature of the Course: Theory + Lab
Semester: V

Full Marks: 60 + 20 + 20
Pass Marks: 24 + 8 + 8
Credit Hrs: 3

Course Description: The course introduces the underlying the principles and design of cryptosystems. The course covers the basics concepts of cryptography including: traditional ciphers, block ciphers, stream ciphers, public and private key cryptosystems. The course also includes the theory of hash functions, authentication systems, network security protocols and malicious logic.

Course Objectives: The objectives of this course are to familiarize the students with cryptography and its applications. The students will be able to develop basic understanding of cryptographic mechanisms.

Course Contents:

Unit I: Introduction and Classical Ciphers (7 hr)

1.1. Security: Computer Security, Information Security, Network Security, CIA Triad, Cryptography, Cryptosystem, Cryptanalysis, Security Threats and Attacks, Security Services, Security Mechanisms

1.2. Classical Cryptosystems:
Substitution Techniques: Ceasar, Monoalphabetic, Playfair, Hill, Polyalphabetic ciphers, One-time pad
Transposition Techniques: Rail Fence Cipher

1.3. Modern Ciphers: Block vs. Stream Ciphers, Symmetric vs. Asymmetric Ciphers

Unit II: Symmetric Ciphers (10 hr)

12.1. Fiestel Cipher Structure, Substitution Permutation Network (SPN)
12.2. Data Encryption Standards (DES), Double DES, Triple DES
12.3. Finite Fields: Groups Rings, Fields, Modular Arithmetic, Euclidean Algorithm, Galois Fields (GF(p) & $GF(2^n)$), Polynomial Arithmetic
12.4. International Data Encryption Standard (IDEA)
12.5. Advanced Encryption Standards (AES) Cipher
12.6. Modes of Block Cipher Encryptions (Electronic Code Book, Cipher Block Chaining, Cipher Feedback Mode, Output Feedback Mode, Counter Mode)

Unit III: Asymmetric Ciphers (8 hr)

13.1. Number Theory: Prime Numbers, Fermat's Theorem, Euler's Theorem, Primility Testing, Miller-Rabin Algorithm, Extended Euclidean Theorem, Discrete Logarithms
13.2. Public Key Cryptosystems, Applications of Public Key Cryptosystems
13.3. Distribution of public key, Distribution of secret key by using public key cryptography, Diffie-Helman Key Exchange, Man-in-the-Middle Attack
13.4. RSA Algorithm
13.5. Elgamal Cryptographic System

Unit IV: Cryptographic Hash Functions and Digital Signatures (8 hr)

14.1. Message Authentication, Message Authentication Functions, Message Authentication Codes
14.2. Hash Functions, Properties of Hash functions, Applications of Hash Functions
14.3. Message Digests: MD4 and MD5
14.4. Secure Hash Algorithms: SHA-1 and SHA-2
14.5. Digital Signatures: Direct Digital Signatures, Arbitrated Digital Signature
14.6. Digital Signature Standard: The DSS Approach, Digital Signature Algorithm
14.7. Digital Signature Standard: The RSA Approach

Unit V: Authentication (3 Hrs)

15.1. Authentication System,
15.2. Password Based Authentication, Dictionary Attacks,
15.3. Challenge Response System,
15.4. Biometric System
15.5. Needham-Schroeder Scheme, Kerberos Protocol

Unit VI: Network Security and Public Key Infrastructure (6 Hrs)

16.1. Overview of Network Security
16.2. Digital Certificates and X.509 certificates, Certificate Life Cycle Management
16.3. PKI trust models, PKIX
16.4. Email Security: Pretty Good Privacy (PGP)
16.5. Secure Socket Layer (SSL) and Transport Layer Security (TLS)
16.6. IP Security (IPSec)
16.7. Firewalls and their types

Unit VII: Malicious Logic (3 Hrs)

7.1. Malicious Logic, Types of Malicious Logic: Virus, Worm, Trojan Horse, Zombies, Denial of Service Attacks,
7.2. Intrusion, Intruders and their types, Intrusion Detection System

Laboratory Works:

The laboratory work includes implementing and simulating the concepts of cryptographic algorithms, hash functions, digital signatures, network security protocols and malicious logic. Students are free to use any of the language and platform as per the skills.

Text Book:

1. W. Stallings, *Cryptography and Network Security*, Pearson Education.

Reference Books:

1. William Stallings, *Network Security, Principles and Practice.*
2. Matt Bishop, *Computer Security, Art and Science*.
3. Mark Stamp, *Information Security: Principles and Practices.*
4. Bruce Schneier, *Applied Cryptography*.
5. Douglas. R. Stinson. *Cryptography: Theory and Practice.*
6. B. A. Forouzan, *Cryptography & Network Security*, Tata Mc Graw Hill.