ICT 3172: INFORMATION SECURITY [3 0 0 3]

Course Objectives:

- To describe the key concepts of information security.
- To infer different cryptographic algorithms along with their evolution.
- To apply the knowledge of mathematics for developing secure cryptosystems.
- To analyze various security mechanisms as well as protocols.

Abstract:

Introduction to Information and Network Security, Symmetric-Key Ciphers: Classical and Modern encryption techniques, Block ciphers, Advanced Encryption Standard, Uses block ciphers, Asymmetric-Key Cryptographic Ciphers, Principles of public key cryptosystems, Number theory concepts, Uses of primes, Message Integrity and Message Authentication, Cryptographic hash functions, Application of cryptographic hash functions, Digital Signature, Key Management, Entity Authentication, Transport Level Security, System Security concepts, Firewalls, Network Intrusion detection and prevention systems.

Syllabus:

Introduction to Information and Network Security
Computer Security Concepts, Security Goals, Security Attacks, Security Services, Security Mechanisms, Security Techniques **[2 Hours]**

Symmetric-Key Ciphers
Kerckhoff’s principle, Substitution ciphers, Transposition ciphers, Stream and block ciphers, DES, AES, Use of modern block ciphers
[8 Hours]

Asymmetric-Key Ciphers
Asymmetric cryptosystems, RSA, Rabin, ElGamal, ECC, Diffie Hellman **[8 Hours]**

Message Integrity and Message Authentication
Message integrity, Random Oracle model, Message authentication, Hash function, SHA-512, Whirlpool **[4 Hours]**

Digital Signature

Digital signature schemes: RSA, ElGamal, Schnorr, ECDS, Digital Signature Standard, Attacks on digital signature
[4 Hours]

Entity Authentication
Passwords, Challenge-response, Zero-knowledge, Biometrics **[1 Hour]**

Key Management
KDC, Kerberos, Public key distribution: Certification Authority, Public Key Infrastructure **[3 Hours]**

Transport Layer Security
TLS/SSL: Architecture, Protocols, Message Formats **[2 Hours]**

System Security
Firewalls, Network Intrusion Detection and Prevention Systems **[4 Hours]**

Course Outcomes:
At the end of this course, the students are able to

- Recall the foundational theory behind information security.
- Understand several basic principles and mathematical techniques used when designing a secure system.
- Apply assorted cryptographic algorithms for providing the core security services.
- Analyze the application of the security mechanisms learnt in various domains.
- Devise suitable cryptosystems for solving real-life security problems in practical systems.

References:

1. William Stallings, *Cryptography and Network Security: Principles and Practice (7e),* Pearson Publications, 2016.
2. Charles P. Pfleeger, Shari Lawrence Pfleeger , Jonathan Margulies, *Security in Computing (5e),* Prentice Hall, 2015.
3. Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security (5e),* Cengage Learning, 2015.
4. Mark Stamp, *Information Security: Principles and Practice (2e),* John Wiley & Sons, 2011.
5. Behrouz A. Forouzan, Debdeep Mukhopadhyay, *Cryptography and Network Security (2e), (Revised),* Tata McGraw-Hill Education India, 2010.