L	T	P	C
3	-	-	3

18BC301 INFORMATION 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:

The student will be able to:

- Understand classical encryption techniques, block and stream cipher encryption techniques.
- Simulate symmetric & asymmetric ciphers and their use in networks.
- Analyze protocols used in Web Security and Transport layer Security.

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…)
- Perform case study with either of the open source tools for network security and analysis.

Syllabus

UNIT – 1 **12 Hours**

NETWORK SECURITY INTRODUCTION: Security Trends – Security attacks – Security services – Security Mechanisms – A Model for Network Security Model

UNIT – 2 **12 Hours**

CLASSICAL ENCRYPTION TECHNIQUES: Symmetric Cipher Model – Substitution Techniques – Caesar cipher-Monoalphabetic cipher-Playfair cipher-Vigenere cipher-Transposition Techniques –Railfence ciphert-transposition cipher

UNIT – 3 **12 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 .

UNIT – 4 **12 Hours**

PUBLIC-KEY ENCRYPTION AND HASH FUNCITONS: Principles of Public –Key Cryptosystems – RSA Algorithm – Key Management.

UNIT – 5 **12 Hours**

Web AND SYSTEM: Security- Secure Electronic Transaction; Intruders – Intrusion Detection – Password Management – Malicious Software - Firewalls.

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.