CSEL 441: FUNDAMENTALS OF CRYPTOGRAPHY

L	T	P	C
3	0	0	3

Prerequisites:

- Basic knowledge of Cryptographic Concepts

Objectives:

- To Learn Mathematical Cryptographic Algorithms
- To Learn Modern Cryptography
- To learn Secure Protocols for Secure Transactions

Outcomes:

- Ability to understand various cryptography concepts.
- Acquiring skills to work with block chain and analyse various cryptographic protocols.

Module-I: Introduction to Cryptography (9 hrs)

History and overview of Cryptography – Introduction to Secure Programming - API's for Secure Programming - Java Cryptography Extension – .Net Cryptography Extension

Module-II: Elementary Number Theory (9 hrs)

Prime numbers, Factoring – Modular Arithmetic – Fermat's & Euler's Theorem – GCD, Euclid's Algorithm – Discrete Logarithm Problem – Implementing all the algorithms and Theorems using JCE/. NCE

Module-III: Modern Cryptography (9 hrs)

Symmetric Key Encryption - Message Integrity – Public Key Cryptography – Digital Signatures – Implementation of DES, RSA, TDES, ECC, IDEA, MD, SHA – Implementing all the algorithms using JCE/. NCE

Module-IV: Financial Cryptography (9 hrs)

Cryptocurrency - Block chain Applications – Contactless Payments and Ticketing Systems – Digital Cash and Payment Systems – Secure banking and Financial Services – Microfinance and Micropayments – Implementation of Cryptocurrency and Block chain using JCE/. NCE

Module-V: Cryptographic Protocols (9 hrs)

SSL/TLS, SSH, TLS, HTTP/HTTPS, IPSEC, P2P, PGP – Security Protocols – Implementation of All Protocols using JCE/. NCE

Text Books:

1. David Hook 'Beginning Cryptography with Java' 2005, ISBN:978-0-7645-9633-9
2. William Stallings, Cryptography and network security, Pearson Education.
3. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Hand- book of Applied Cryptography, CRC Press.