MCA (2020-2022)
Trimester IV
Cyber Security

117P05C401	Cyber Security	3-0-0	3-0-0	3

Objectives:

The major objective of this course is to understand key terms and concepts in cyber law, and cybercrimes, various forms authentications and cryptographic algorithms such as public key cryptographic algorithm, secret key cryptographic algorithm etc. The learner will develop an understanding of security policies (such as confidentiality, integrity, and availability), as well as protocols to implement such policies. Learners are introduced to various defense techniques and wireless and mobile security mechanisms.

Contents:

- **Introduction to Cyber Security:** Overview of Cyber Security, Security mind-set , Security Attacks, Security Services and Security Mechanisms, CIA triad, Types of cybercrimes, IT ACT 2000, National Cyber Security Policy 2013

- **Encryption & Hashing:**
  Secret Key Cryptography: Block Encryption, DES rounds, S- Boxes IDEA: overview, comparison with DES, Key expansion, IDEA rounds.
  Public Key Cryptography: Introduction to modular arithmetic, RSA, Digital Signature, Deffie-Hellman Key Exchange, Elliptic Curve Cryptography.
  Hash Functions and Message Digests: MD2, MD5, SHA

- **Access Control:** Types of Authentication- Password-based authentication, address-based authentication, cryptographic authentication, smart cards, biometrics, mutual authentications, reflection attacks, KDC-working, multi domain KDC

- **Digital Certificates and Public Key Infrastructure:** Digital Certificate- creation, verification, Certificate revocation, Cross-certification, Certificate Hierarchy, Internet Security Protocols: SSL, SET, Email Security- PGP, PEM, S/MIME, IPSec

- **Firewall and Intrusion detection System:** Introduction to Firewalls, its types**,** Intrusion Detection: Methods and Modes, Response, Detection mechanism

- **Wireless & Mobile Security:** Wireless security, Wireless network threats, Wireless network measures, mobile device security, security threats, mobile device security strategy.
- **Text Books:**
- Principles of Computer Security , Wm. Arthur Conklin, Gregory White, Dwayne Williams, Roger L. Davis & Chuck Cothren, McGraw Hill Education
- Cryptography and Network Security: Principles and Practice, Willam Stallings, Prentice Hall.
- Cryptography & Network Security, Behrouz A Forouzan, McGraw-Hill.

Reference Books:

- Cybersecurity for beginners, Raef Meeuwisse, Hythe, Kent : Cyber Simplicity.

- Certified Ethical Hacker Practice Exams, MATT WALKER, McGrawHill Education.