MCA505A-CRYPTOGRAPHY AND CYBER LAW

Module – 1 Introduction - Cyber Attacks, Defence Strategies and Techniques, Guiding Principles, Mathematical Background for Cryptography - Modulo Arithmetic's, The Greatest Common Divisor, Useful Algebraic Structures, Chinese Remainder Theorem
Basics of Cryptography - Preliminaries, Elementary Substitution Ciphers, Elementary Transport Ciphers, Other Cipher Properties, Secret Key Cryptography – Product Ciphers, DES Construction.

Module – 2 Public Key Cryptography and RSA – RSA Operations, Why Does RSA Work?, Performance, Applications, Practical Issues, Public Key Cryptography Standard (PKCS), Cryptographic Hash - Introduction, Properties, Construction, Applications and Performance, The Birthday Attack, Discrete Logarithm and its Applications - Introduction, Diffie-Hellman Key Exchange, Other Applications.

Module – 3 Key Management - Introduction, Digital Certificates, Public Key Infrastructure, Identity–based Encryption, Authentication–I - One way Authentication, Mutual Authentication, Dictionary Attacks, Authentication – II – Centralized Authentication, The Needham-Schroeder Protocol, Kerberos
Intrusion Prevention and Detection - Introduction, Prevention Versus Detection, Types of Instruction Detection Systems, DDoS Attacks Prevention/Detection,
Web Service Security – Motivation, Technologies for Web Services, WS- Security, SAML, Other Standards.

Module –4
Concepts of Cyber Crime and the IT ACT-2000,Hacking,Teenage Web Vandals,Cyber Fraud and Cyber Cheating,Nature of Cyber criminality,Strategies to tackle cyber crime and trends,Criminal justice in India and implications on Cyber Crime
Copyright Ownership and Assessment,License of CopyRight,CopyRight Term and respect for foreign Work,Copy Right Infringement,Remedies and Offers,Computer Software piracy

TextBooks:
1. Cryptography, Network Security and Cyber Laws – **Bernard Menezes**, Cengage Learning, 2010
2.Cyber Law simplified- **VivekSood**, Mc-GrawHill, 11th reprint , 2013

Reference Books:
1. Cryptography and Network Security- Behrouz A Forouzan, DebdeepMukhopadhyay, Mc-GrawHill, 3rd Edition, 2015
2. Cryptography and Network Security- William Stallings, Pearson Education, 7th Edition