

MSCS304 INFORMATION SECURITY (3-0-0)

Module-I (9Hrs)

The Security Problem in Computing: The meaning of computer Security, Computer Criminals, Methods of Defense; Elementary Cryptography: Substitution Ciphers, Transpositions, Making “Good” Encryption Algorithms, Private-Key Cryptosystems, The Data Encryption Standard, The AES Encryption Algorithm, Public-Key Cryptosystems, Public Key Encryptions, Uses of Encryption, Pseudo-randomness, and Hashing.

Module-II (9Hrs)

Program Security :Secure Programs, Non-malicious Program Errors, viruses and other malicious code, Targeted Malicious code, controls Against Program Threats, Protection in General-Purpose operating system protected objects and methods of protection memory and address protection, File protection Mechanisms, User Authentication Designing Trusted O.S : Security polices, models of security, trusted O.S. design, Assurance in trusted OS, Implementation examples. Digital Signatures, Authentication, Secret Sharing, Group oriented cryptography, Identification.

Module-III (9Hrs)

Data base & Network Security: Security requirements, Reliability and integrity, Sensitive data, Inference, multilevel database, proposals for multilevel security; Security in Network; Threats in Network, Network Security Controls, Firewalls, Intrusion Detection Systems, Secure E-mail.

Module-IV (9Hrs)

Administering Security: Security Planning, Risk Analysis, Organizational Security policies Physical Security; The Economics of Cyber security; Privacy in Computing; Legal and Ethical Issues in Computer Security: Protecting Programs and data, Information and the law, Rights of Employees and Employers, Software failures, Computer Crime, Case studies of Ethics.

Textbooks:

1. Charles P. Pfleeger & Shari Lawrence Pfleeger, “Security in Computing”, Fourth Edition, 2007, Pearson Education, Inc. New Delhi. Pvt. Ltd., New Delhi.
2. William Stallings & Lawrie Brown, “Computer Security: Principles and Practice”, First Edition, 2008, Pearson Education, New Delhi.

Reference Books

1. Charlie Kaufman, Radia Perlman & Mike Speciner, “Network Security: Private Communication in a Public World”, 2nd Edition, 2003, PHI Learning. New Delhi.
2. Chuck Easttom, “Computer Security Fundamentals”, First Edition, 2006, Pearson Education, Inc. New Delhi.