INT888:CYBER SECURITY

L:3 T:0 P:0 Credits:3

Course Outcomes: Through this course students should be able to

CO1 :: Recognize basic concepts in information security, including security policies, security models and security mechanisms for improving the security of computing systems

CO2 :: Interpret highest professional and ethical standards of conduct, including impartiality and the protection of personal privacy

CO3 :: Examine the requirements and techniques for security management, risk analysis and controls

CO4 :: Utilize the knowledge related to various cyber laws and related semantics for deploying security mechanisms

Unit I

Introduction to Cyber Security : what does secure mean, attacks, the meaning of computer security, methods of defense, encryption overview, elementary cryptography terminology and background, substitution ciphers, transposition, making good encryption algorithm

Unit II

Security In Networks : network concept, threats in networks, network security controls, firewall, Intrusion detection systems, secure e-mail

Unit III

Database and Data Mining Security : Introduction to databases, security requirements, reliability and integrity, sensitive Data, Inference, data mining

Unit IV

Administering Security and its economics : Security Planning, Risk Analysis, Organizational Security Policies, Physical Security, Quantifying Security, Modeling Cybersecurity

Unit V

Privacy in Computing : Privacy Concepts, Privacy Principles and Policies, Authentication and Privacy, Data Mining, Privacy on the Web, E-Mail Security

Unit VI

legal and ethical issues in Computer Security : protecting programs and data, Information and the law, ethical issues in computer security, quantifying security, current research and future direction, case studies of ethics, Computer Crime

Text Books:

1. SECURITY IN COMPUTING by CHARLES P. PFLEEGER, SHARI LAWRENCE PFLEEGER, PEARSON

References:

1. NETWORK SECURITY AND CRYPTOGRAPHY by BERNARD MENEZES, CENGAGE LEARNING