

CSAOEUG(E)-INFORMATION SECURITY BASICS

CREDIT 3 : LTP (2:0:1)

Course Objectives

- To Prepare Students to understand Security basics
- Understand Cryptography and comprehensive study of the principles and practices of computer system security
- Understand operating system security, network security, software security and web security.
- Understand common attacking techniques such as virus, trojan, worms and common security policies and the basic cryptography.
- Understand ethical issues in computer security.

Unit Wise Syllabus:

UNIT - I

Introduction Security, Attacks, Computer Crime, Security Services, Security Mechanisms, Cyber Crimes, Information Technology ACT, Cryptography, Substitution Ciphers, Transpositions Cipher, Block Cipher, Stream Cipher

UNIT - II

Confusion, Diffusion, Symmetric key, Asymmetric key, Encryption, DES Algorithm, Hash function, Digital Signatures, Digital Certificates.

UNIT-III

Program Security, Program Errors, Malicious Codes, Virus, Trapdoors, Salami Attacks, Threats, Covert channels, Control Against program, Program Security issues, Protecting Programs.

Protection in OS: Memory and Address Protection, Access control, File Protection, User Authentication.

UNIT-IV

Database Security, Requirements, Reliability, Integrity, Sensitive Data, Inference, Multilevel Security, Types of Crimes, Ethical issues in Security, Protecting data.

UNIT-V

Security in Networks, Threats in Networks, Security Controls, firewalls, Intrusion detection systems, Secure e-mails, Administrating Security, Security Planning, Risk Analysis, Organisational Security Policy, Physical Security.

Expected Outcomes

The students shall be able to understand

- The common threats faced today,
- Foundational theory behind information security,
- The basic principles and techniques when designing a secure system.
- Attacks and defenses work in practice,

Revised copy (in summs from 3)