R-15

IV B.Tech II Semester

15ACS81-INFORMATION SECURITY

L	T	P	C
3	1	0	3

Course Objectives:

1. *To introduce students with basic concepts in information system and its relevance in modern society.*
2. *To understand several security requirements and operations - analysis, design, and implementation of the Security System Development Life Cycle (SecSDLC)*
3. *To understand and implement authentication, integrity and confidentiality along with related protocols*

Prerequisites:

Computer networks, software engineering

UNIT- I:

Introduction

History, critical characteristics, components, approaches of implementation, security systems development life cycle, security professionals.

Security Issues:

Need for security, threat, risk, attack, legal and ethical issues.Legal, Ethical and Professional Issues: law and ethics in information security, relevant u.s laws-international laws and legal bodies, ethics and information security.

UNIT- II

Security technology-firewalls and VPNs: physical design, firewalls, protecting remote connections.Planning for security: security policy, standards and practices, security blue print, security education, continuity strategies.

UNIT- III

Security technology-intrusion detection: access control and other security tools - intrusion detection and prevention systems, scanning and analysis tools, biometric access controls.**Cryptography:** foundations of cryptology, cipher methods, cryptographic algorithms, cryptographic tools, protocols for secure communications, attacks on cryptosystems.

UNIT- IV

Electronic mail security:

Pretty Good Privacy (PGP); S/MIME

Security tools:

Intrusion detection systems, honey pots, honey nets and padded cell systems, scanning and Analysis tools.

UNIT- V

Implementing information security: information security project management, technical topics of implementation, non-technical aspects of implementation, security certification and accreditation.

Security and personnel: positioning and staffing security function, credentials of information security professionals, internal control strategies.

Information security maintenance: security management models, the security maintenance model, digital forensics.

Course Outcomes:

1. *Aware of information security issues and understand its technologies.*
2. *Able to discover, analyse and deal with threads using advanced security issues and technologies.*
3. *Understand the current legal issues towards information security.*

TEXT BOOKS:

1. Michael e. Whitman, h j mattord , 2nd edition principals of information security,Thompson course technology, 2007.
2. Michael e. Whitman and hebert j mattord, “principles of information security”, fourth edition, cengage learning 2011.
3. Behrouz a forouzan, debdeepmukhopadhyay, cryptography and network security, 2nd Edition, tatamcgraw hill education private limited , new delhi, 2012.

REFERENCES:

1. Thomas r peltier, justingpeltier, john blackley, “information security fundamentals”, auerbacj publications 2010.
2. Detmar w straub, seymorgoodman, richard l baskerville, “information security policy proceses and practices”, phi, 2008.
3. Marks merkow and jimbreithaupt, “information security principle and practices”, pearson education, 2007.
4. Kaufman, perlman , speciner ‘network security’ phi ,india, 2nd ed. 2010
5. **Online references** : http://www.cryptogram.org