**Title of Subject : Information Security (SW-316)**

**Discipline :** Software Engineering (5th Semester)

**Effective :** 17 Batch & onwards

**Pre-requisite :** Computer Networks

**Assessment :** Theory**:** 20% Sessional, 80% Written Semester Examination

## (20% Mid, 60% Final)

**Credit Hours :** 03 + 00 **Marks:** 100

**Minimum Contact Hours:** 45

# Specific Objectives of course:

* To become better IS professional or to enhance their Knowledge of information security.
* To learn detailed working of the DES, Quantum Cryptography and different Internet security Protocol.
* To gain knowledge of enterprise level security with different hardware and software security solution.
* To gain knowledge of web application security program in organization.
* To learn about important mechanisms to assess weakness in the network and IT infrastructure that can be exploited by attackers.

**COURSE LEARNING OUTCOMES:**

Upon successful completion of the course, the student will be able to:

|  |  |  |  |
| --- | --- | --- | --- |
| **CLOs** | **Description** | **Taxonomy level** | **PLO** |
| 1 | Explain the concept and knowledge of IS and implementation of cryptography and related techniques using information security concepts. | C1 | 1 |
| 2 | Analyze enterprise level security by using different hardware and software Security solutions. | C4 | 2 |
| 3 | Use Information security solution for an organization in order to cope with their security issues. | C3 | 3 |

**PROGRAM LEARNING OUTCOMES (PLOs):**

The course is designed so that students will achieve the following PLOs:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Engineering Knowledge: | ☑ | 7 | Environment and Sustainability: | ☐ |
| 2 | Problem Analysis: | ☑ | 8 | Ethics: | ☐ |
| 3 | Design/Development of Solutions: | ☑ | 9 | Individual and Team Work: | ☐ |
| 4 | Investigation: | ☐ | 10 | Communication: | ☐ |
| 5 | Modern Tool Usage: | ☐ | 11 | Project Management: | ☐ |
| 6 | The Engineer and Society: | ☐ | 12 | Lifelong Learning: | ☐ |

**Course outline:**

* **Introduction to Information Security**

Course Introduction, Three Objectives of IT Security, Three Foundations of IT Security, Introduction to Classical Cryptography, The Threat Environment, Basic Security Terminology, Traditional External Attackers, Classic Malware: Viruses and Worms, Trojan Horses and Rootkits, Hackers, Social Engineering used by Hackers

* **Cryptography**

Definitions & Concepts, Kerckhoff's Principle, Strength of the Cryptosystem, Services of Cryptosystems, Methods of Encryption, Symmetric Cryptography, Asymmetric Cryptography, Symmetric vs Asymmetric Algorithms, Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Blowfish, RC4, RC5, RC6, Review of Cryptography

* **Encryption**

# Link Encryption vs End-to-End Encryption, Encryption at Different Layers, Hardware vs Software Cryptography Systems, Email Standards, Quantum Cryptography, Internet Security, Enterprise Network Architecture, Different Traffic Flows in the Enterprise, Implementing Security in the Enterprise, Internet Protocols

* **Firewalls**

Firewalls, Types of Firewalls, Types of Firewalls, Firewall Configurations and Demilitarized Zone (DMZ), Distributed Firewalls , Intrusion Detection and Prevention System (IDPS),IPS Technologies, IPS Response Techniques, Common IPS Detection Methodologies, System and Server Security

* **Web Application Security**

Information Security Assessments, Technical Assessment Techniques, Testing Viewpoints, Vulnerability Scanning, Target Vulnerability Validation Techniques, Penetration Testing Overview and Phases,

* **Layer-2 Security**

Security Features on Switches, Layer 2 Security, Types of Layer 2 Attacks, Port Level Traffic Controls, Spanning Tree Protocol (STP) Features, Access Control Lists on Switches, Layer 2 Security Best Practices, Twenty Critical Security Controls, Award-winning Security Products

# Recommended Books:

1. Corporate Computer and Network Security by Raymond Panko, Prentice Hall, Latest Edition.
2. CISSP, Shon Harris, McGraw-Hill Osborne Media, Latest Edition.
3. Cryptography and Network Security, William Stallings, Prentice Hall, Latest Edition.

|  |  |  |
| --- | --- | --- |
| **Approval:** |  | |
| **Board of Studies:** | **Resolution No. 02** | **Dated: 29-08-2019** |
| **Board of Faculty:** | **Resolution No. 01** | **Dated: 07-10-2019** |
| **Academic Council:** | **Resolution No. 96.10** | **Dated: 07-10-2019** |