Lok Jagruti Kendra University
University with a Difference

# Diploma in Computer Engineering

LJ Polytechnic

## Course Code: 025020507

## Web & Network Security

| Programme / Branch Name | | | Diploma in Computer Engineering | | | |
|---|---|---|---|---|---|---|
| **Course Name** | Web & Network Security | | | | **Course Code** | 025020507 |
| **Course Type** | HSSC | BSC | ESC | PCC | OEC | PEC |

**Legends:** HSSC: Humanities and Social Sciences Courses BSC: Basic Science Courses
ESC: Engineering Science Courses PCC: Program Core Courses
OEC: Open Elective Courses PEC: Program Elective Courses

## 1. Teaching and Evaluation Scheme

| Teaching Hours / Week / Credits | | | | Evaluation Scheme | | | |
|---|---|---|---|---|---|---|---|
| **L** | **T** | **P** | **Total Credit** | **CCE** | **SEE (Th)** | **SEE (Pr)** | **TOTAL** |
| 3 | 0 | 4 | 5 | 50 | 50 | 50 | 150 |

**Legends:**
L: Lectures T: Tutorial P: Practical
CCE: Continuous & Comprehensive Evaluation
SEE (Th): Semester End Evaluation (Theory)
SEE (Pr): Semester End Evaluation (Practical)
SEE (Pr): Semester End Evaluation (Practical)

## 2. Prerequisites

- ✓ Basics of information technology
- ✓ Concepts of network and email security

## 3. Rationale

This course provides the foundation to upgrade the key issues associated with protecting information assets over a network. This course covers basic cryptography concepts, techniques and encryption algorithms. The purpose of the course is to provide the student with an overview of the field of information as well as web security and assurance in handling the information threats.

## 4. Objectives

- ✓ The theory should be taught and practical should be carried out in such a manner that students are able to acquire different learning outcomes in cognitive, psychomotor and affective domain to demonstrate following course outcomes.
  - Identifying the web threat types.
  - Intrusion detection techniques to tackle the threat.
  - Data transmission with cryptography techniques.

## 5. Contents

| Unit No. | Topics | Sub-Topic | Learning Outcomes | % Weightage | Hours |
|---|---|---|---|---|---|
| **1** | **Introduction to Information Security** | 1.1 Overview of information security<br>1.2 Security services and mechanisms<br>1.3 Security attacks<br>1.4 Model for network security<br>1.5 Cryptography<br>1.6 Cryptanalysis<br>1.7 Symmetric cipher model<br>1.8 Asymmetric cipher model | • To get knowledge about various types of attacks in network<br>• To understand symmetric & asymmetric cipher | 10 | 06 |
| **2** | **System Security** | 2.1 Cryptographic substitution techniques<br>2.2 Cryptographic transposition techniques<br>2.3 Diffie Hellman key exchange algorithm<br>2.4 Limitations of Symmetric encryption<br>2.5 Steganography<br>2.6 Euclidean algorithm using divisibility algorithm | • Understanding about cryptographic techniques<br>• Understand types of Cryptography<br>• Understand steganography | 30 | 10 |
| **3** | **Cryptography Techniques** | 3.1 Block cipher principle<br>3.2 Fiestal structure<br>3.3 First round of DES<br>3.4 Applications of asymmetric cryptography<br>3.5 Requirements for asymmetric cryptography<br>3.6 RSA algorithm: Description and explanation with block diagram | • To know block cipher encryption<br>• To understand applications of cryptography<br>• To understand RSA algorithm for block encryption | 20 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| **4** | **MAC and HASH Functions** | 4.1 Cryptography application: HASH function<br>4.2 Requirements of hash function<br>4.3 MD5 hashing<br>4.4 SHA overview<br>4.5 MAC: introduction and requirements | • To understand hashing and its functions<br>• To understand types of hashing algorithms | 10 | 06 |
| **5** | **Web Security Applications** | 5.1 Digital Signature: Definition and properties<br>5.2 PGP: description, confidentiality and authentication<br>5.3 General format of PGP<br>5.4 S/MIME: MIME content type, S/MIME functions<br>5.5 Secure Socket Layer protocol<br>5.6 Secure Electronic Transaction protocol<br>5.7 Intrusion Detection Techniques<br>5.8 Firewall: Definition and types of firewall | • To understand applications of asymmetric cryptography: Digital Signature<br>• To understand applications of web security: PGP, S/MIME, SET | 30 | 10 |
| | | | | **Total Hours** | **42** |

## 6. List of Practicals / Exercises

The practical/exercises should be properly designed and implemented in an attempt to develop different types of skills so that students can acquire the competencies/program outcomes. Following is the list of practical exercises for guidance.

| Sr. No | Practical / Exercises | Key Competency | Hours |
|---|---|---|---|
| 1 | Prepare a report on cryptanalysis. | To analyze the cryptanalysis concept | 04 |
| 2 | Write a program to perform encryption of plain text using Caesar cipher. | To analyze the use of Caesar cipher encryption | 02 |
| 3 | Write a program to perform encryption of a plain text using Playfair cipher. | To analyze the use of Playfair cipher encryption | 04 |
| 4 | Write a program to perform encryption of a plain text using Hill cipher. | To analyze the use of Hill cipher encryption | 04 |

| | | | |
|---|---|---|---|
| 5 | Generate an executable file from a C compiler and generate its Message Digest Sum (MD5). Note Down the MD5. | To analyze the use of C compiler (MD5) | 02 |
| 6 | Generate an executable file from a C compiler and Generate its secure hash algorithm (SHA 256, SHA 512). Note down the SHA Values. | To analyze the use of c compiler algorithm SHA 256 & 512 | 02 |
| 7 | Change the above C program with a minor modification and again generate its executable. Check the SHA256 and SHA512 of the new file. Verify the SHA values of both the files. | To analyze the use of C compiler algorithm modification SHA 256 & 512 value files | 02 |
| 8 | Change the above C program with a minor modification and again generate its executable. Check the SHA256 and SHA512 of the new file. Verify the SHA values of both the files. | To analyze the use of C compiler algorithm SHA256 and 512 value files | 02 |
| 9 | Configure firewall of (Win XP/ Win 7). | To understand the fundamental security system of Windows | 04 |
| 10 | Install Wireshark tool for packet capture. | To understand and analyze the key features of an application that capture and analyze the data packet flowing through a network | 04 |
| 11 | Inspect IP packets and identify source and destination IP using the Wireshark tool. | To understand IP packets | 02 |
| 12 | Download Avast free AV or Clam AV open source. Check the updates of the anti-malware. Identify your operating system. Update the OS and identify updates. | To learn the use of fundamental anti malware applications that are used to detect threat | 04 |
| 13 | Inspect the firewall at your department in CWN. Understand its functionality, identify the important configuration parameters for the same. | To understand firewall | 04 |
| 14 | Understand MAC implementation. | To understand MAC | 04 |
| 15 | Implement RSA cipher. | To understand RSA cipher | 04 |
| 16 | Understand DES cipher implementation. | To understand DES cipher | 04 |
| 17 | Prepare a Chart and/or presentation on SSL Protocol Stack. | To know SSL stack | 02 |
| 18 | Prepare a chart / model to explain the importance of Digital Signature. | To understand Digital Signature | 02 |
| | | **Total Hours** | **56** |

## 7. Suggested specification Table with hours

| Unit No. | Chapter Name | Teaching Hours | Distribution of Topics According to Bloom's Taxonomy | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | R % | U % | App % | C % | E % | An % |
| 1 | Introduction to information security | 06 | 40 | 50 | - | - | - | 10 |
| 2 | System security | 10 | 20 | 30 | 5 | - | 40 | 5 |
| 3 | Cryptography techniques | 10 | 35 | 25 | 10 | - | 10 | 20 |
| 4 | MAC and HASH functions | 06 | 10 | 40 | 5 | 5 | 20 | 20 |
| 5 | Web security applications | 10 | 25 | 35 | 20 | 5 | 5 | 10 |

**Legends:** R: Remembering U: Understanding
App: Applying C: Creating
E: Evaluating An: Analyzing

## 8. Text Books

1) "Cryptography and Network Security" by Fourozon, Pearson publication
2) Cryptography and Network Security Principles and Practices, Atul Kahate [Tata-McGraw-Hill]
3) Network Security: Private Communication in a Public World,CharlieKaufman
4) Cryptography Theory and Practice,Douglas R. Stinson

## 9. Reference Books

1) "Network Security Essentials" by William Stallings, Pearson publication
2) "Cryptography: An Introduction" by Nigel Smart, Tata McGraw Hill publication

## 10.Open Sources (Website, Video, Movie)

1) https://www.md5summer.org/download.html
2) https://www.tutorialspoint.com/network_security/index.html
3) https://www.tutorialspoint.com/webservices/web_services_security.html
4) https://www.edx.org/learn/cryptography
5) https://www.coursera.org/learn/crypto