# Th-1 CRYPTOGRAPHY & NETWORK SECURITY

COMMON TO (CSE/IT)

| | | | |
|---|---|---|---|
| **Theory** | **4 Periods per week** | **Internal Assessment** | **20 Marks** |
| **Total Periods** | **60 Periods** | **End Sem Exam** | **80 Marks** |
| **Examination** | **3hours** | **Total Marks** | **100Marks** |

**A. Topic wise distribution of periods**

| **Sl. No.** | **Topics** | **Periods** |
|---|---|---|
| 1 | POSSIBLE ATTACKS ON COMPUTERS | 05 |
| 2 | CRYPTOGRAPHY CONCEPTS | 10 |
| 3 | SYMMETRIC & ASYMMETRIC KEY ALGORITHMS | 15 |
| 4 | DIGITAL CERTIFICATE & PUBLIC KEY INFRASTRUCTURE | 10 |
| 5 | INTERNET SECURITY PROTOCOLS | 10 |
| 6 | USER AUTHENTICATION | 04 |
| 7 | NETWORK SECURITY & VPN | 06 |
| | **TOTAL** | **60** |

**B. RATIONALE**

Now a day almost all It related jobs use the internet as the backbone service. Therefore it is highly essential for an IT professional to have a fare idea on the security aspect of internet service. This paper aims to provide the student with the various security threats in internet and discuss the different techniques to implement this. One of such technique is implementation of cryptography in the confidential data to be floated in the internet.

**C. OBJECTIVE**: After completion of this course the student will be able to**:**

- Understand the basic concepts that of security approach.
- Learn about different attack on the computer systems.
- Learn about the measures to save computer hardware and software.
- Understand different certification to ensure security.
- Learn about basic concepts of firewalls and their use.
- Understand privacy and security.

**D. DETAIL CONTENTS:**

1. **Possible attacks on Computers**

   1.1 The need for security
   1.2 Security approach
   1.3 Principles of security
   1.4 Types of attacks

2. **Cryptography Concepts**

   2.1 Plain text & Cipher Text
   2.2 Substitution techniques
   2.3 Transposition techniques

2.4 Encryption & Decryption
2.5 Symmetric & Asymmetric key cryptography

**3. Symmetric & Asymmetric key algorithms**

3.1 Symmetric key algorithm types
3.2 Overview of Symmetric key cryptography
3.3 Data encryption standards
3.4 Over view of Asymmetric key cryptography
3.5 The RSA algorithm
3.6 Symmetric & Asymmetric key cryptography
3.7 Digital signature

**4. Digital certificate & Public key infrastructure**

4.1 Digital certificates
4.2 Private key management
4.3 PKIX Model
4.4 Public key cryptography standards

**5. Internet security protocols**

5.1 Basic concept
5.2 Secure socket layer
5.3 Transport layer security
5.4 Secure Hyper text transfer protocol(SHTTP)
5.5 Time stamping protocol (TSP)
5.6 Secure electronic transaction (SET)

**6. User authentication**

6.1 Authentication basics
6.2 Password
6.3 Authentication Tokens
6.4 Certificate based authentication
6.5 Biometric authentication

**7. Network Security & VPN**

7.1 Brief introduction of TCP/IP
7.2 Firewall
7.3 IP Security
7.4 Virtual Private Network (VPN)

**Coverage of Syllabus upto Internal Exams (I.A.)**
**Chapter 1,2,3,4**

**BOOKS Recommended:-**

| Sl.No | Name of Authors | Title of the Book | Name of the publisher |
|---|---|---|---|
| 01 | A. Kahate | Cryptography & Network security | TMH |
| 02 | W.Stallings | Cryptography & Network Security Principals and Practices | Prentice Hall |
| 03 | Pachghare | Cryptography & Information security | PHI |