# GUJARAT TECHNOLOGICAL UNIVERSITY, AHMEDABAD, GUJARAT

## COURSE CURRICULUM
## COURSE TITLE: ESSENTIALS OF INFORMATION SECURITY
## (COURSE CODE: 3351602)

| Diploma Program in which this course is offered | Semester in which offered |
|---|---|
| Information Technology | 5th Semester |

## 1. RATIONALE

The objective of Information Security is to upgrade fundamentals of security over network. This course covers basic cryptography concepts, techniques and encryption algorithms. After going through this course student will be able to configure security policy in OS.

## 2. COMPETENCIES

The course content should be taught and implemented with the aim to develop different types of skills so that students are able to acquire following competencies:

- **Explain basics of Information Security.**
- **Identify and explain functioning of various Encryption Algorithms.**

## 3. COURSE OUTCOMES:

The theory should be taught and practical should be carried out in such a manner that students are able to acquire different learning out comes in cognitive, psychomotor and affective domain to demonstrate following course outcomes.

i. Describe importance of Security in Communication.

ii. Explain basic concept of Encryption Algorithm.

**iii.** Identify Firewall Techniques.

**iv.** Explain latest trends in OS Security Assessment Tools .

## 4. TEACHING AND EXAMINATION SCHEME

| Teaching Scheme (In Hours) | | | Total Credits (L+T+P) | Examination Scheme | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | Theory Marks | | Practical Marks | | Total Marks |
| L | T | P | C | ESE | PA | ESE | PA | 200 |
| 3 | 0 | 4 | 7 | 70 | 30 | 40 | 60 | |

**Legends: L** - Lecture; **T** - Tutorial/Teacher Guided Student Activity; **P** - Practical; **C** - Credit; **ESE** - End Semester Examination; **PA** - Progressive Assessment

## 5. COURSE DETAILS

| Unit | **Major Learning Outcomes** (in cognitive domain) | **Topics and Sub-topics** |
|---|---|---|
| **Unit – I**<br><br>**Introduction of Information Security** | 1a.Explain various concepts related to Information Security | 1.1 Need of Information Security<br>1.2 Security Trends<br>1.3 What is Information Security<br>1.4 Overview of Information Security<br>1.5 Security Services<br>1.6 Security Mechanism<br>1.7 Security Attacks<br>1.8 The OSI Security Architecture<br>1.9 A Model for Network Security |
| **Unit – II**<br><br>**System Security** | 2a. Symmetric Key Cryptography | 2.1 Symmetric Cipher Model<br>2.2 Cryptography<br>2.3 Cryptanalysis |
| | 2b. Classical Encryption Techniques | 2.4 Substitution Techniques<br>2.4.1 Caesar Cipher<br>2.4.2 Monoalphabetic Cipher<br>2.4.3 Polyalphabetic Cipher<br>2.4.4 Playfair Cipher<br>2.4.5 Hill Cipher<br>2.5 Problems with Symmetric Cipher Algorithms<br>2.6 Diffie-Hellman Key exchange algorithm<br>2.5 Transposition Techniques<br>2.6 Steganography |
| **Unit – III Basic Arithmetics in Encryption** | 3a. Basic Concept in Number theory and finite fields | 3.1 Divisibility and The Division Algorithm<br>3.2 The Euclidean Algorithm<br>3.3 Modular Arithmetic<br>3.4 Random Number<br>3.4 Groups, Rings, and Fields<br>3.5 Finite Fields of the Form GF(p) |
| **Unit – IV Symmetric Encryption Algorithm** | 4a.Block Cipher | 4.1 Block Cipher Principal |
| | 4b Data Encryption Standard, Block cipher modes | 4.2 The Data Encryption Standard<br>4.3 Fiestel Structure<br>4.4 First Round of DES<br>4.5 Strength of DES<br>4.5.1 Double DES<br>4.5.2 Man in the Middle Attack<br>4.6 Block Cipher Modes of Operation<br>4.6.1 Electronic Code Book<br>4.6.2 Cipher Block Chaining Mode<br>4.6.3 Cipher Feedback Mode |

| Unit | Major Learning Outcomes (in cognitive domain) | Topics and Sub-topics |
|---|---|---|
| | | 4.6.4 Output Feedback Mode<br>4.6.5 Counter Mode |
| **Unit - V Asymmetric Key Encryption** | 5a.Symmetric encryption | 5.1 Limitations of Symmetric Key Encryption |
| | 5b.Asymmetric encryption | 5.2 Asymmetric Key Encryption<br>5.2.1 Maintaining Confidentiality<br>5.2.2 Maintaining Authentication<br>5.2.3 Managing confidentiality and authentication together |
| **Unit- VI Operating System Security** | 6a. Configuration OS Security | 6.1 Windows OS Hardening<br>6.1.1 Configure Security Policy<br>6.1.2 Configure Firewall (Win XP, Win 7) |
| | 6b .Anti virus Approach | 6.2 Anti Malware and Cleanup Tools<br>6.2.1 Windows AVG<br>6.2.2 ClamAV (Open source)<br>6.2.3 Avast |
| | 6c. Security Assessment | 6.3 OS Security Assessment Tools<br>6.3.1 Nessus (Windows, Linux)<br>6.3.2 SAINT (Linux, Open Source) |
| | 6.d Windows Updates | 6.4 OS Updates<br>6.4.1 Windows Patches<br>6.4.2 Windows Upgrades<br>6.4.3 Linux Updates, upgrades |

**6. SUGGESTED SPECIFICATION TABLE WITH HOURS & MARKS (THEORY)**

| Unit No. | Unit Title | Teaching Hours | Distribution of Theory Marks | | | |
|---|---|---|---|---|---|---|
| | | | R Level | U Level | A Level | Total Marks |
| I | **Introduction of Information Security** | 06 | 4 | 4 | 2 | 10 |
| II | **System Security** | 10 | 4 | 6 | 2 | 16 |
| III | **Basic Arithmetic in Encryption** | 06 | 2 | 6 | 4 | 08 |
| IV | **Symmetric Encryption Algorithm** | 08 | 4 | 4 | 4 | 16 |
| V | **Asymmetric Key Encryption** | 06 | 4 | 4 | 6 | 10 |
| VI | **Operating System Security** | 06 | 4 | 4 | 2 | 10 |
| | **Total** | **42** | **22** | **28** | **20** | **70** |

**Legends:** R = Remembrance; U = Understanding; A = Application and above levels (Revised Bloom's taxonomy)

**Note:** This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

## 7. SUGGESTED LIST OF EXERCISES/PRACTICAL

The practical/exercises should be properly designed and implemented with an attempt to develop different types of skills **(outcomes in psychomotor and affective domain)** so that students are able to acquire the competencies/programme outcomes. Following is the list of practical exercises for guidance.

***Note**: Here only outcomes in psychomotor domain are listed as practical/exercises. However, if these practical/exercises are completed appropriately, they would also lead to development of certain outcomes in affective domain which would in turn lead to development of **Course Outcomes** related to affective domain. Thus over all development of **Programme Outcomes (**as given in a common list at the beginning of curriculum document for this programme) would be assured.*
*Faculty should refer to that common list and should ensure that students also acquire outcomes in affective domain which are required for overall achievement of Programme Outcomes/Course Outcomes.*

| Sr. No. | Unit No. | Practical Exercises (Outcomes in Psychomotor Domain) | Hrs. required |
|---|---|---|---|
| 1 | I | To study various Security Trends and Security services. | 4 |
| 2 | | To study various Security Attacks and Security Mechanism. | 2 |
| 3 | | To study OSI Security Architecture.. | 2 |
| 4 | II | To study various Cryptographic Technique. | 4 |
| 5 | | To study cryptanalysis. | 4 |
| 6 | III | To study and perform encryption of a plain text and decryption of cipher text using one time pad method | 4 |
| 7 | | To study and perform encryption of plain text and decryption of cipher text of a using caesar cipher. | 4 |
| 8 | | To study and perform encryption of a plain text and decryption of cipher text using Monoaplhabetic cipher. | 4 |
| 9 | | To study and perform encryption of a plain text and decryption of cipher text using play fair cipher. | 2 |
| 10 | | To study and perform decryption of a cipher text using polyalphabetic cipher | 2 |
| 11 | | To study and perform encryption of a plain text and decryption of cipher text using rectangular cipher | 4 |
| 12 | | To study and perform encryption of a plain text and decryption of cipher text using columnar cipher | 4 |
| 13 | | To study and perform encryption of a plain text and decryption of cipher text using Hill cipher | 4 |
| 14 | IV | To study block cipher modes of operation. | 2 |
| 15 | | To study single round of DES. | 2 |
| 16 | V | To study Asymmetric encryption. | 2 |

| Sr. No. | Unit No. | Practical Exercises (Outcomes in Psychomotor Domain) | Hrs. required |
|---|---|---|---|
| 17 | VI | To study and configure Security in OS (Win XP / Win 7) | 4 |
| 18 | | To study and configure firewall of (Winx XP/ Win 7) | 4 |
| Total Hours (practical for 56 hours from above representing each unit may be selected) | | | 58 |

## 8. SUGGESTED LIST OF STUDENT ACTIVITIES

Following is the list of proposed student activities such as:

i. **Seminar with power point presentation**

ii. **Design a model of Network Security**

## 9. SPECIAL INSTRUCTIONAL STRATEGIES (if any)

i. Assignment can be given based on above topics.
ii. Student can

## 10. SUGGESTED LEARNING RESOURCES

### A) List of Books

| S. No. | Title of Book | Author | Publication |
|---|---|---|---|
| 1 | Cryptography and Network Security: Principles and Practice | William Stallings | Prentice Hall |
| 2 | Cryptography: An Introduction | Nigel Smart | Mcgraw-Hill College |
| 3 | Cryptography and Network Security | Forouzan | McGraw Hill |
| 4 | Network Security Essentials | William Stallings | Pearson |
| 5 | Network Security Tools: Writing, Hacking, and Modifying Security Tools - See more | Justin Clarke, Nitesh Dhanjani | O'Reilly Media; |
| 6 | Network Security | Atul Kahate | Tata McGraw Hill |
| 7 | Cryptography and Security in Computing | Jaydip Sen | In Tech |

### B) List of major equipment with major Specification

- **Desktop computer P-IV processor or higher**
- **LINUX**

### C) List of Software/Learning Websites

**Web sites :**

- www.**cryptography**.com
- **http://searchsecurity.techtarget.com**
- cse.iitkgp.ac.in/

**Electronic Teaching Slides (Power Point Slides)- CD/DVD**

- **Data Encryption Standard**
- **Feistel Structure**
- **Block cipher modes of Operation**

**Laboratory Charts**

- **Security Attacks**
- **Security Mechanisms**
- **OSI Security Architecture**

## 11. COURSE CURRICULUM DEVELOPMENT COMMITTEE

**Faculty Members from Polytechnics**

- **Prof PARVEZ K. FARUKI, In charge Head ( IT ), BPTI, Bhavnagar**
- **Prof MANOJ P. PARMAR, In charge Head ( IT ), G. P. Himatnagar.**
- **Prof. MANISH D. PATEL , In charge Head ( IT ), R C T I Ahmedabad**
- **Prof SUNIL PARYANI, Lecturer , IT , G P Himatnagar**
- **MS. DARSHANA TRIVEDI, Lecturer, IT, RCTI, Ahmedabad**

- **Coordinator and Faculty Members from NITTTR Bhopal**

1) **Dr. M. A. Rizvi,** Associate Professor, Dept. of Computer Engineering and Applications.
2) **Dr. R. K. Kapoor**, Associate Professor, Dept. of Computer Engineering and Applications, NITTTR.