# Charotar University of Science and Technology (CHARUSAT)
# Faculty of Technology and Engineering (FTE)

## Subject: Fundamentals of Information Security (ITUE205) (Elective-I)

## Semester: 4th

### Teaching Scheme:

| Teaching Scheme | Theory | Practical | Tutorial | Total | Credit |
|---|---|---|---|---|---|
| Hours/Week | 4 | 2 | - | 6 | 5 |
| Marks | 100 | 50 | - | 150 | |

### Course Pre-requisites:

- Computer Networks and Internet Protocol: https://nptel.ac.in/courses/106105183

### Course Description:

This course provides a foundation in information security concepts, including cryptographic techniques, network security, system security, and emerging threats. It emphasizes both theoretical understanding and hands-on implementations.

### Course Objectives:

1. To develop a strong mathematical foundation for cryptographic techniques and security algorithms.
2. To explore symmetric and asymmetric cryptographic techniques for secure communication.
3. To understand message authentication, hash functions, and digital signatures for ensuring data integrity and authenticity.
4. To provide insights into system security, malware threats, firewalls, and internet privacy solutions like VPNs and Tor.
5. To encourage self-study and research-oriented learning through real-world security implementations and case studies.

### Course Outcomes:

By the end of the course, students will be able to:

1. **CO1:** Apply the concepts of different techniques to implement security goals and security mechanisms.
2. **CO2:** Apply the different encryption and decryption algorithms using symmetric & asymmetric approaches to provide data confidentiality.
3. **CO3:** Apply the integrity and authentication aspects, like digital signature and message digest, and map them with practical use.
4. **CO4:** Apply web application, network, and system security to make them immune to attack.

- **Pre-requisites online video / course:**
  - Computer Networks and Internet Protocol, Prof. S. Ghosh and Prof. S. Chakraborty, IIT Kharagpur: https://nptel.ac.in/courses/106105183

- **Self-study/Further Study components and materials:**

| **Unit No.** | **Unit/Topic Details** | |
|---|---|---|
| 1 | **MATHEMATICAL FOUNDATIONS FOR INFORMATION SECURITY** | |
| | 1.1 | Practical applications of Number Theory in cryptography |
| | 1.2 | Understanding Modulo Operations and its role in encryption |
| | 1.3 | Hands-on with OpenStego / OpenPuff for Steganography |
| | **Materials**:<br>➢ https://math.mit.edu/research/pure/number-theory.html#:~:text=Number%20theory%20has%20applications%20in,the%20arithmetic%20of%20K3%20surfaces<br>➢ https://embeddedsw.net/OpenPuff_Steganography_Home.html | |
| 2 | **SYMMETRIC KEY CIPHERS** | |
| | 2.1 | Comparative study: DES vs AES security |
| | 2.2 | Hands-on: Implementing AES encryption in Python |
| | 2.3 | Exploring Modes of AES Operations with practical examples |
| | **Materials**:<br>➢ https://www.khanacademy.org/computing/computer-science/cryptography<br>➢ https://www.youtube.com/watch?v=O4xNJsjtN6E | |
| 3 | **PUBLIC KEY CRYPTOGRAPHY** | |
| | 3.1 | Comparing RSA, ECC, and ElGamal cryptography |
| | 3.2 | Generating RSA Key Pairs using OpenSSL |
| | 3.3 | Understanding Public Key Infrastructure (PKI) and Certificates |
| | **Materials**:<br>➢ https://www.gpgfrontend.bktus.com/extra/algorithms-comparison/#:~:text=Use%20Cases%3A%20ElGamal%20is%20used,RSA%20or%20ECC%2Dbased%20methods<br>➢ https://www.ibm.com/think/topics/public-key-infrastructure#:~:text=Public%20key%20infrastructure%20(PKI)%20provides,%2C%20integrity%2C%20nonrepudiation%20and%20authenticity | |
| 4 | **MESSAGE AUTHENTICATION & HASH FUNCTIONS** | |
| | 4.1 | Hash Collisions: Understanding how MD5 vulnerabilities led to real-world attacks |
| | 4.2 | Hands-on: Generate SHA-256, SHA-512 hashes in Python |
| | 4.3 | Digital Signature verification using OpenSSL |
| | **Materials**:<br>➢ https://www.youtube.com/watch?v=b4b8ktEV4Bg<br>➢ https://aruljohn.com/blog/python-sha-md5-hash/ | |

## Syllabus:

| Unit No. | Unit/Topic Details | | Hours (hr) | Evaluation Weightage (%) |
|---|---|---|---|---|
| 1. | **BASIC CONCEPTS OF INFORMATION SECURITY** | | 05 | 8.33 |
| | 1.1 | Introduction to Information Security: Terminologies, Goals of Information Security | | |
| | 1.2 | Implementation Issues of the Goals of Information Security | | |
| | 1.3 | Control Mechanisms for Information Security | | |
| | 1.4 | Access Control - Administrative and Technical | | |
| | 1.5 | Passwords - Are they secure? | | |
| | 1.6 | Passwords, Hash Function, Common Password Threats | | |
| | 1.7 | Multifactor Authentication – Challenges | | |
| | 1.8 | Spheres of Information Security | | |
| 2. | **INTRODUCTION AND MATHEMATICAL FOUNDATIONS FOR INFORMATION SECURITY** | | 12 | 20 |
| | 2.1 | Security Goals, Security trends - Attacks, Services and Mechanisms | | |
| | 2.2 | Classical Encryption techniques (Mono-alphabetic, Poly-alphabetic substitution techniques and Transposition techniques) Overview of steganography along with demo tools like OpenPuff Tool, OpenStego, etc. | | |
| | 2.3 | Number Theory - Prime And Relative Prime Numbers, Modular Arithmetic, Congruence, Fermat and Euler's theorem, Euclid's Algorithm, Chinese Remainder theorem | | |
| 3. | **SYMMETRIC KEY CIPHERS** | | 15 | 25 |
| | 3.1 | Simplified Data Encryption Standard | | |
| | 3.2 | Data Encryption Standard (DES), Triple DES | | |
| | 3.3 | Block Cipher Principles | | |
| | 3.4 | Characteristics of Advanced Symmetric Block Cipher | | |
| | 3.5 | Block Cipher Design Principles | | |
| | 3.6 | Advanced Encryption Standard Algorithm (AES) | | |
| | 3.7 | Modes of Operations (Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode & Counter Mode) | | |
| 4. | **PUBLIC KEY CRYPTOGRAPHY** | | 9 | 15 |
| | 4.1 | Principles of Public-Key Cryptography | | |
| | 4.2 | Public Key Cryptography Standards (PKCS) | | |
| | 4.3 | RSA Algorithm | | |
| | 4.4 | Key Management | | |
| | 4.5 | ElGamal Algorithm | | |
| | 4.6 | Diffie-Hellman Key Exchange | | |
| | 4.7 | Elliptic Curve Cryptography (ECC) | | |
| 5. | **MESSAGE AUTHENTICATION AND HASH FUNCTION** | | 11 | 18.33 |
| | 5.1 | Message Authentication | | |
| | 5.2 | Hash Functions | | |
| | 5.3 | Message Authentication Code (MAC) | | |

|  |  |  |  |  |
|---|---|---|---|---|
|  | 5.4 | Security of Hash Functions And MAC |  |  |
|  | 5.5 | Secure Hash Algorithm (SHA) |  |  |
|  | 5.6 | Hash-Based Message Authentication Code (HMAC) |  |  |
|  | 5.7 | Digital Signatures, Types of Digital Signature: RSA, Elgamal |  |  |
| 6. | **SYSTEM SECURITY, INTERNET PRIVACY WITH PROXIES, VPNS AND TOR** |  | 8 | 13.34 |
|  | 6.1 | Malware, Functions of Malware, Sources of Malware, Layers of Defense Against Malware |  |  |
|  | 6.2 | Firewall Characteristics, Capabilities and Limitations, Types of Firewalls (Packet Filtering, Stateful Packet Inspection, Application Proxy & Circuit-level Proxy) |  |  |
|  | 6.3 | System administration and security, ufw UNIX firewall |  |  |
|  | 6.4 | Packet Capture demo using tools like Tcpdump, Wireshark, etc. |  |  |
|  | 6.5 | Wireless Network, Security Threats, Public Networks & Administering Wireless |  |  |
|  | 6.6 | Internet Privacy with Proxies, VPNs and Tor, |  |  |
|  | 6.7 | Recent Research Papers on Security |  |  |
|  |  | **Total:** | **60** |  |

***Course Articulation Matrix:***

|  | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 | PSO1 | PSO2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CO1 | 3 | 2 | 1 | 1 | - | 1 | - | 1 | 1 | - | - | - | 1 | 2 |
| CO2 | 3 | 3 | 3 | 2 | 3 | 1 | - | - | - | - | - | - | 1 | 1 |
| CO3 | 2 | 2 | 3 | 2 | 3 | 2 | - | - | 2 | 1 | - | - | 1 | 1 |
| CO4 | 3 | 3 | 3 | 2 | 3 | - | 2 | 1 | 2 | 1 | 1 | 2 | 3 | 3 |

The correlation levels 1, 2 or 3 are as defined below:
1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High), If there is no correlation, put "-" placed.

***Recommended tools used:***

1. Penetration Testing: Kali Linux, Parrot Security OS
2. Steganography: Steghide, StegoSuite, Xiao Steganography
3. Footprinting & OSINT: OSINT Framework
4. Port Scanning: Nmap
5. Cryptography & Encryption: OpenSSL, CrypTool
6. Vulnerability Assessment: OpenVAS
7. Password Recovery: Passware, Advanced Archive Password Recovery, Advanced PDF Password Recovery
8. Hashing & Data Integrity: HashCalc, MD5 Calculator
9. Firewall Security: Various firewall software solutions (to be evaluated)
10. Network Traffic Analysis: Wireshark, TCPdump

***Recommended Study Material:***

- **Textbooks:**

1. William Stallings, “Cryptography and Network Security Principles and Practice”, 8th Edition – Pearson (2023).
2. Behrouz A. Forouzan, “Cryptography and Network Security”, 3rd Edition - McGraw Hill Education (2015).

- **Reference Books:**

1. Atul Kahate, “Cryptography and Network Security”, 4th Edition - The McGraw-Hill Companies (2019).
2. William Stallings, “Network Security Essentials: Applications And Standards”, 6th Edition - Pearson Education (2018).
3. Douglas Robert Stinson, “Cryptography: Theory and Practice”, 4th Edition - CRC Press (2018).

***Online Resources:***

1. Introduction to Information Security I, IIT Madras
   Link: https://nptel.ac.in/courses/106106129
2. Cryptography, Information Security
   Link:
   https://www.youtube.com/playlist?list=PLc4vStPmkiS6JPVys1KZ0UtSQDXu5ibNM
3. Ethical Hacking Essentials (EC-Council)
   Link: https://charusat.edu.in/ilms/course/view.php?id=157
4. Network Defense & Ethical Hacking
   Link: https://charusat.edu.in/ilms/course/view.php?id=159

***Practical/Lab Work Implementation:***

- **Penetration Testing OS Selection**: Evaluate and install the most suitable penetration testing OS (Kali Linux vs Parrot Security OS) based on user requirements, user-friendliness, and hardware requirements.
- **Steganography Implementation:** Use tools like Steghide, StegoSuite, and Xiao Steganography to conceal/hide secret files and messages in other file formats.
- **Footprinting & OSINT:** Gather target information using the OSINT Framework to analyze vulnerabilities and reconnaissance techniques.
- **Port Scanning with Nmap:** Perform scanning and enumeration using Nmap to detect open ports and services in a network.
- Implement public key encryption like RSA/ECC/Diffie Hellman for secure data transfer using OpenSSL.
- **Vulnerability Assessment with tools like OpenVAS:** Conduct vulnerability scanning of networks using OpenVAS and analyse security risks.
- **Password Recovery Techniques:** Recover encrypted passwords from applications using tools like Passware, Advanced Archive Password Recovery, and Advanced PDF Password Recovery.

- **Hash Verification for Data Integrity:** Generate and compare hash values using HashCalc and MD5 Calculator to ensure data integrity.
- **Cryptographic Analysis using tools like CrypTool:** Explore cryptographic algorithms and analyze their strengths using CrypTool.
- **Firewall Security Testing**: Evaluate and compare different firewall software solutions for securing network traffic.
- **Network Analysis:** Capture and analyze network traffic using tools like Wireshark or TCPdump etc.

***Care Taking Points:***

- **Clarification of Self-Study Topics:** Doubts arising from self-study topics will be addressed and clarified during classroom sessions to ensure comprehensive understanding.
- **Case Study-Based Pedagogy:** Case study-based learning will be the primary teaching method to provide practical exposure and hands-on problem-solving experience in security.
- **Hands-On Learning:** Practical exercises, real-world case studies, and projects will form an essential part of the course to help students apply theoretical knowledge to practical situations.
- **Industry-Relevant Tools and Techniques:** Students will work with industry-standard tools and technologies to develop the skills to solve real-world data security problems.
- **Regular Assessments:** To track progress, continuous assessment will be conducted through quizzes, assignments, case studies, presentations, and research or project work.
- **Expert/Guest Lectures:** Interaction with industry experts through guest lectures, webinars, or workshops will offer insights into the latest trends and applications in security.