1. Name of the Course: Computer Security

2. LTP structure of the course: L:2 T:1 P:1

3. Objective of the course: This course provides an essential study of Computer Security issues and methods of overcoming those issues. These include system/software vulnerabilities, applied cryptography, host-based security, Operating system based security and hardware security. Also provides, hands on experience to show complication of not following security principle.

4. Outcome of the course: After successful completion of this course, students will be familiar with the different computer security concepts in the theoretical and practical perspective.

5. Course Plan: As per the below format only

Component	Unit	Topics for Coverage	Chapter No. (Optional)
Component 1	Unit 1	Introduction to Computer Security: Threats, Attacks, User Identification Authentication, Access Control Confidentiality, Integrity and Availability Security threats: DoS, Trojan Horse, Virus, Worms, Backdoors, Brute Force, Password Crack, Spoofing, Man in the Middle Attack, Sniffing, keyloggers, Overflow attacks and BadUSB, Virtual Machine and Honeypot.	
	Unit 2	Cryptography: Symmetric Key Encryption (DES), Asymmetric Key encryption (RSA), Hash functions, Digital Signature, Public Key Infrastructure (PKI) and Digital Certificate.	
Component 2	Unit 3	Security Module: TPM, Sandboxing and Isolation, OS security (access control), IDS, Firewall, Anti-Virus. Mobile OS security.	
	Unit 4	Web Security: SQLi, CSS, CSRF. Network Security: TLS and IPSec, DNSSec. Introduction to Side Channel Analysis.	

6. Text Book:

> William Stallings, Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall, 3rd edition

7. References:
- Gerardus Blokdyk, Mobile Operating System Security A Complete Guide - 2021 Edition
- Additional references of papers will be provided by the Instructor.