Semester	7
Program	B.Sc. Computer Science (Hons.)
Course	SECURITY AND PRIVACY
Paper Code	C4CS230731T
No. of Credits	4
Hours / week	Theory: 4
Category: Core/MDC/SEC/VAC	Core
Theory/ Practical / Composite	Theory
Number of Modules	Two
Course Overview: This course provides a comprehensive introduction to the fundamental principles of computer security and cryptography with an overview of security concepts, including various types of attacks, roles of intruders and essential security services and mechanisms used to protect information systems. The course also explores the objectives and foundations of cryptography, covering both symmetric key and asymmetric key algorithms, along with block and stream ciphers. Students are expected to gain an understanding of cryptanalysis techniques and their importance in evaluating the strength of cryptographic systems. Further, the course addresses authentication mechanisms, including password-based systems, challenge-response techniques and biometric authentication methods. It also introduces the concept of digital certificates and their role in secure communication.	
Course Outcomes	**CO1.** Explain basic security concepts including attacks, computer criminals, security services, and mechanisms **CO2.** Describe and apply cryptographic principles including block and stream ciphers, and differentiate between private key and public key algorithms **CO3.** Analyze cryptographic systems and evaluate their vulnerabilities using basic cryptanalysis techniques **CO4.** Identify secure programming practices and analyze non-malicious errors and malicious codes such as viruses, worms, Trojan horses, and trapdoors **CO5.** Explain network security threats and implement security controls such as firewalls **CO6.** Apply various authentication techniques including password-based systems, challenge-response mechanisms, and biometric authentication **CO7.** Explain the role of digital certificates and evaluate their use in ensuring secure communication **CO8.** Analyze security features and vulnerabilities within network protocol suites
Syllabus	

Unit/ Module	Content	Hours	CO Mapping	Cognitive Level
GROUP A				
1	Security, Attacks, Computer Criminals, Security Services, Security Mechanisms	5	CO1	K2 (Understand)
2	Objectives, Block Ciphers and Stream Ciphers, Private Key and Public Key Cryptography Algorithms, Cryptanalysis	12	CO2, CO3	K3, K4 (Apply, Analyze)
3	Secure programs, Non-Malicious Program errors, Malicious codes Virus, Worms and Trojan Horses, Trap doors	9	CO4	K4 (Analyze)
GROUP B				
4	Threats in security of networks, security controls, firewalls	6	CO5	K3 (Apply)
5	Definition of entity authentication, password technique, challenge response technique and biometric authentication process, digital certificate	14	CO6	K3 (Apply)
6	Security in network protocol suite	6	CO7, CO8	K4 (Analyze)

Text Books

1. Cryptography and Network Security by B.A.Forouzan, McGraw-Hill Publication

2, Cryptography and Network Security – Principles and Practice by William Stallings, PHI Publication

3. Cryptography and Network Security by Atul Kahate, McGraw-Hill Publication

Suggested Readings

1. Cryptography Theory and Practice by D.R.Stinson, Chapman & Hall/CRC

Web Resources

1. NPTEL course on Internetwork Security by Prof. Sourav Mukhopadhyay, IIT Kharagpur; course link: https://youtu.be/1plMO7ChXMU?si=NAOKLJzCmnyCbBBy

Evaluation	Theory CIA: 25 Attendance: 5 Semester Exam: 70

Paper Structure for Theory Semester Exam Module:
Answer 5 out of 7 of 7 marks each in Group A
Answer 5 out of 7 of 7 marks each in Group B

Course outcomes (COs) and Cognitive Level Mapping

COs	CO Description	Cognitive Levels
CO1	Security concepts & attacks	K2 (Understand)
CO2	Cryptographic techniques	K3 (Apply)
CO3	Cryptanalysis	K4 (Analyze)
CO4	Software security and malware	K4 (Analyze)
CO5	Network security controls	K3 (Apply)
CO6	Authentication techniques	K3 (Apply)
CO7	Digital certificates	K4 (Analyze)
CO8	Network protocol security	K4 (Analyze)