Semester	**7**
Course	**MAJOR**
Paper Code	
Paper Title	**SECURITY AND PRIVACY**
No. of Credits	**4**
Theory / Practical / Composite	**THEORY**
Minimum No. of preparatory hours per week a student has to devote	**5**
Number of Modules	**TWO**
Syllabus	**Group A** 1. Security, Attacks, Computer Criminals, Security Services, Security Mechanisms 2. Objectives, Block Ciphers and Stream Ciphers, Private Key and Public Key Cryptography Algorithms, Cryptanalysis 3. Secure programs, Non-Malicious Program errors, Malicious codes Virus, Worms and Trojan Horses, Trap doors **Group B** 4. Threats in security of networks, security controls, firewalls 5. Definition of entity authentication, password technique, challenge response technique and biometric authentication process, digital certificate 6. Security in network protocol suite
Learning Outcomes	1. To make students understand the concepts of security threat in any network communications and in data storage 2. To impart the knowledge of the fundamental algorithms on encryption and decryption 3. To give an overview on different security policies 4. To learn cryptographic techniques 5. To learn symmetric key and asymmetric key cryptosystems 6. To understand the importance of key distribution in network protocol
Reading/Reference Lists	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
Evaluation	Theory CIA: 25 Attendance: 5 Semester Exam: 70
Paper Structure	GROUP A: Answer 5 out of 7 of 7 marks each GROUP B: Answer 5 out of 7 of 7 marks each