# 20IT32P2 - CRYPTOGRAPHY AND NETWORK SECURITY LABORATORY

|  |  |  |  |
| --- | --- | --- | --- |
| Course Category: | Professional Core | Credits: | 1.5 |
| Course Type: | Practical | Lecture-Tutorial-Practical: | 0-0-3 |
| Prerequisite: | Knowledge in Computer Fundamentals and Basic Mathematical Fundamentals. | Sessional Evaluation:  Univ. Exam Evaluation:  Total Marks: | 40  60  100 |
| Objectives: | * To learn and practice the essentials of Encryption and Decryption Procedure of Cryptography. | | |

|  |  |  |
| --- | --- | --- |
| Course Outcomes | Upon successful completion of the course, the students will be able to: | |
| CO1 | Understand the basics of Encryption and Decryption Procedure of Cryptography. |
| Course Content | 1. Write a Program for Caesar Cipher in Substitution Techniques. 2. Write a Program for Playfair Cipher in Substitution Techniques. 3. Write a Program for Hill Cipher in Substitution Techniques. 4. Write a Program for One-Time pad in Substitution Techniques. 5. Write a Program for RSA. 6. Write a Program for S-DES Algorithm. 7. Write a Program for Diffie-Hellman Algorithm. 8. Write a Program for El Gamal Cryptosystem. | |
| Text Books &  Reference  Books | **TEXT BOOKS:**   1. Cryptography and Network Security: Principles and Practice-William Stallings, 6th Edition, Prentice Hall   **REFERENCE BOOKS:**   1. Network Security Essentials (Applications and Standards) by William Stallings, Pearson Education. 2. Fundamentals of Network Security, by Eric maiwald. 3. Principles of Information Security by Whitman, Thomson. 4. Network Security - The Complete Reference by Robert Bragg | |