|  |  |  |  |
| --- | --- | --- | --- |
| **Course Code** | IT352 | **Course Name** | Information Assurance and Security |
| **Core/Elective/ML C:** | Core | **L-T-P** | 3-0-2 |
| **Pre-requisites:** | Fundamentals of Computer Networks | **Contact Hours:** | 9:00 am to 5:30 pm |
| **Type of course: (Lecture/Tutorial**  **/Seminar/Project)** | Lecture | **Course Assessment Methods:**  **(both continuous and semester-end assessment)** | 1. Mid Term : 25M  2. End Term : 45M  3. Mini project : 20M  4. Announced test(2) : 10M |
| **Course Objectives:**   * CO1: To understand the basic concepts of Information Security and its usage. * CO2: Understanding the basic security applications and mechanisms used to protect information. * CO3: Understanding the fundamentals of Cryptography and its usage in computer networks with the   applications   * CO4: Understanding vulnerabilities, threats and risks in Information Security. * CO5: Understanding the concepts of System Security Policies. | | | |

Texts and References

1. William Stallings, Cryptography and Network Security, Fourth Edition, Pearson Education/PHI, 2003.
2. Micheal E. Whitman and Herbert J. Mattord principles of information Security, 2nd Edition, Thomson, 2005.
3. Atul Kahate , Cryptography and Network Security, Tata McGrawHill, 2003.
4. Behrouz A. Forouzan: Cryptography and Network Security, Tata McGrawHill, 2007.

|  |  |  |
| --- | --- | --- |
| SI No | Weeks | Topics covered |
| 1 | 1 – 3 | **Introduction to Information Security:** Need for computer Security, Basics concepts, Security attributes, Security goals and violations, Security policies and procedures. |
| 2 | 4 - 7 | **Cryptography:** Introduction, Symmetric ciphers, Symmetric key cryptography, Public key cryptography and RSA key management. |
| 3 | 8 - 9 | **Public key cryptography and Hash functions**: Message authentication and Hash functions, Hash and MAC algorithms, Digital signature and authentication protocols. |
| 4 | 9 - 10 | **Security attacks:** Different types of attack and its existing solutions. |
| 5 | 11 - 12 | **Network Security Applications:** Authentication applications, IP Security, Web Security. |
| 6 | 13- 14 | **System Security:** Intruders, Malicious Software, Firewalls, Analysis of security tool. |

**Course Instructor**

Ganesh Murgod