# 20IT3202 - CRYPTOGRAPHY AND NETWORK SECURITY

|  |  |  |  |
| --- | --- | --- | --- |
| Course Category: | Professional Core | Credits: | 3 |
| Course Type: | Theory | Lecture-Tutorial-Practical: | 3-0-0 |
| Prerequisite: | Knowledge in Computer security basics and counter attack mechanisms from Internet Threats. | Sessional Evaluation:  Univ. Exam Evaluation:  Total Marks: | 40  60  100 |
| Objectives: | * Understand OSI security architecture and classical encryption techniques. * Acquire fundamental knowledge on the concepts of finite fields and number theory. * Understand various block cipher and stream cipher models. * Describe the principles of public key cryptosystems, hash functions, digital signature and internet security. | | |

|  |  |  |
| --- | --- | --- |
| Course Outcomes | Upon successful completion of the course, the students will be able to: | |
| CO1 | Understand the basics of Computer Security and conventional encryption issues. |
| CO2 | Know the different types of Data Encryption models of Symmetric Cipher Techniques and required basic number theory. |
| CO3 | Gain the knowledge in Data Encryption models of Advanced Symmetric Cipher Techniques. |
| CO4 | Learn and able to design different types of Data Encryption models of Asymmetric Cipher Techniques and required basic number theory. |
| CO5 | Study the Data Integrity, authentication protocols and classification of digital signature standards. |
| CO6 | Acquire the knowledge of Mutual Trust with Internet-related security mechanisms. |
| Course Content | UNIT-I  **Introduction**: Overview of Computer Security, Security Attacks, Security Services, Security Mechanisms, and a Model for Network Security.  **Classical Encryption Techniques:** Symmetric Cipher Model**,** Substitution Techniques, Steganography.  UNIT-II  **Block Ciphers and the Data Encryption Standard:** Block Cipher Principles, DES, Strength of DES.  UNIT-III  **Advanced Encryption Standard**: The Origins AES, AES Structure, AES Round Functions, AES Key Expansion  **Block Cipher Operation:** Electronic Codebook Mode, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, Counter Mode.  UNIT-IV  **Number Theory:** Prime and Relatively Prime Numbers, Fermat’s and Euler’s theorems, Testing for Primality.  **Public Key Cryptography:** Principles of Public-key Cryptosystems, The RSA Algorithm, Diffie-Hellman Key exchange.  UNIT-V  **Cryptographic Hash Functions:** Applications of Cryptographic Hash Functions, Secure Hash Algorithm (SHA)  **Message Authentication Codes:** Message Authentication Requirements, Message Authentication functions, Message Authentication Codes.  UNIT-VI  **Key Management and Distribution:** Symmetric key Distribution using Symmetric Encryption, Symmetric key Distribution using Asymmetric Encryption, Distribution of Public Keys. | |
| 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. | |
| E-Resources | 1. [WilliamStallings.com/Crypto/Crypto5e.html](http://WWW.WilliamStallings.com/Crypto/Crypto5e.html) 2. [www.Tutorialspoint.com](http://www.Tutorialspoint.com) | |