17CS3103 - CRYPTOGRAPHY AND NETWORK SECURITY

|  |  |  |  |
| --- | --- | --- | --- |
| **Course Category:** | Program 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 and digital signature. | | |

|  |  |  |
| --- | --- | --- |
| **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 | Analyze the models for internet security and learning different types of modern algorithms and its classification. |
| CO3 | Study different methods of public key cryptosystems and its real-time implementation |
| CO4 | Learn different message authentication codes and basics of hash functions |
| CO5 | Study authentication protocols and classification of digital signature standards |
| CO6 | Deal with Internet related security and system security mechanisms. |
| **Course Content** | UNIT – I  **Introduction**: Overview of Computer Security, Security Attacks, Security Mechanisms and Security Services. Model for Network Security, Network Access Security Model.  **Conventional Encryption:** Symmetric Cipher Model**,** Classical Encryption Techniques and Steganography.  UNIT – II  **Modern Techniques:** Block Cipher Principles, S-DES, DES, Strength of DES, AES, Block Cipher Modes of Operation.  **Number Theory:** Prime numbers, Modular arithmetic, Fermat’s and Euler’s theorems, Testing for Primality, Euclidean Algorithm, Chinese Remainder Theorem, and Discrete Logarithms.  UNIT – III  **Public Key Cryptography:** Principles of Pseudorandom Number Generation, Key Distribution & Management, RSA Algorithm, Diffie-Hellman Key exchange, Elliptic Curve Cryptography.  UNIT – IV  **Hash Functions:** Introduction and concepts, Applications**,** Security of Hash functions, Secure Hash Algorithms.  **Message Authentication Codes:** Message Authentication Requirements and functions, Security of MACs, MAC based on Hash Functions and Block Ciphers, Message Digest Algorithm.  UNIT – V  Digital Signatures: Digital signature concept & Applications, Digital signature standards.  User Authentication: Remote User Authentication, Kerberos, X.509 directory service.  **UNIT – VI**  **Web Security**: Web Security requirements, Secure socket layer and Transport layer Security, HTTPS, SSH, Secure Electronic Transaction.  **IP Security:** Overview, Encapsulating Security Payload, Internet Key Exchange.  **System Security:** Intruders, Viruses and Related threats. Fire wall Design Principles, Trusted systems. | |
| **Text Books and References:** | **Text Books:**   1. Cryptography and Network Security: Principles and Practice-William Stallings, Pearson Education. 2. Network Security Essentials (Applications and Standards) by William Stallings, Pearson Education.   **Reference Books:**   1. Fundamentals of Network Security, by Eric maiwald 2. Principles of Information Security by Whitman, Thomson. 3. Network Security - The Complete Reference by Robert Bragg. | |
| **E-Resources** | 1. WilliamStallings.com/Crypto/Crypto5e.html 2. www.Tutorialspoint.com | |