|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | 13CS1105 | - | CRYPTOGRAPHY & NETWORK SECURITY | | | | | | | | |
|  |  | |  | | | | |
| Hours / Week | : | 4 | |  | Sessional Marks | : | 40 |
| Credits | : | 4 | |  | End Examination Marks | : | 60 |

|  |
| --- |
| **UNIT - I** |
| **Fundamentals - Introduction:** OSI security architecture, Security Attacks, Services and Mechanisms, Model for network Security.  **Conventional Encryption:** Conventional Encryption model, Steganography, Classical Encryption Techniques, Placement of Encryption function, Traffic Confidentiality.  **Modern Techniques:** Cipher Principles, Feistel Cipher structure, Data Encryption Standard, Strength of DES, triple DES, Block Cipher design, principles and Modes of Operations, AES-Evaluation criteria for AES. |
|  |
| **UNIT – II** |
| **Public Key Cryptography:** Key management & Distribution, Diffie- Hellman key exchange, Elliptic curve Cryptography, Public key cryptography and RSA.  **Number theory:** Prime and Relatively prime numbers, Modular arithmetic, Fermat’s and Euler’s theorems, Test for primality, Euclid’s Algorithm, Chinese remainder theorem, Discrete logarithms. |
|  |
| **UNIT – III** |
| **Authentication and Hash Function:** Authentication requirements, Authentication functions, Message authentication Code, Hash functions, Security of hash functions and MACs, MD5 Message Digest algorithm , Secure hash algorithm, HMAC, Digital signatures, Authentication protocols, Digital signature standard. |
|  |
| **UNIT – IV** |
| **Network Security:** Authentication applications, Kerberos , X.509 Authentication service , Electronic mail security, PGP, S/MIME.  **IP Security:** Overview, Architecture, Authentication, Encapsulating Security Payload, Combining security Associations.  **Web Security:** Web Security requirements, Secure socket layer and Transport layer security, Secure Electronic Transaction. |
|  |
| **UNIT – V** |
| **System Level Security:** Intruders, Intrusion detection, Password management, Malicious Software: Viruses and related threats, Virus counter measures.  **Firewall:** Need for Firewall & Characteristics, Types of Firewalls, Firewall design principles, Firewall Configuration, Trusted systems. |
|  |
| TEXT BOOKS |
| 1. Cryptography and Network Security: Principles and Practice-William Stallings, Pearson Education. |
| 1. Network Security Essentials (Applications and Standards) by William Stallings, Pearson Education. |