|  |  |  |  |
| --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
| 13CS3202 | - | CRYPTOGRAPHY & NETWORK SECURITY |

 |
|  |  |  |
| Hours / Week | : | 4 |  | Sessional Marks | : | 40 |
| Credits | : | 4 |  | End Examination Marks | : | 60 |

|  |
| --- |
| **UNIT - I** |
| **Introduction**: Attacks, Services and Mechanisms, Security attacks, Security services, A Model for Internetwork Security. Classical Techniques. **Conventional Encryption**: Conventional Encryption model, steganography, Classical Encryption Techniques, Placement of Encryption function.**Modern Techniques**: Simplified DES, Block Cipher Principles, Data Encryption Standard, Strength of DES, triple DES, Block Cipher Design Principles and Modes of operations. |
|  |
| **UNIT – II** |
| **Public Key Cryptography**: Key distribution, Random Number Generation. Traffic confidentiality, RSA Algorithm, Principles, Key Management, Diffie-Hellman Key exchange, Elliptic Curve Cryptography. |
|  |
| **UNIT – III** |
| **Number theory**: Prime and Relatively prime numbers, Modular arithmetic, Fermat’s and Euler’s theorems, Testing for primality, Euclid’s Algorithm, the Chinese remainder theorem, Discrete logarithms. **Message authentication and Hash functions**: Authentication requirements and functions, Message Authentication, Hash functions, Security of Hash functions and MACs. |
|  |
| **UNIT – IV** |
| **Hash and Mac Algorithms**: MD File, Message Digest Algorithm, Secure Hash Algorithm, H MAC. **Digital signatures and Authentication protocols**: Digital signatures, Authentication Protocols, Digital signature standards. Authentication Applications: Kerberos, X.509 directory Authentication service. |
|  |
| **UNIT - V** |
| **IP Security**: Overview, Architecture, Authentication, Encapsulating Security Payload, Combining security Associations, Key Management.**Web Security**: Web Security requirements, Secure sockets layer and Transport layer security, Secure Electronic Transaction. Intruders, Viruses and Related threats. Fire wall Design Principles, Trusted systems. |
|  |
|  |
| 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 Ericmaiwald
2. Principles of Information Security by Whitman, Thomson.
3. Network Security - The Complete Reference by Robert Bragg.