## 3IT02: INFORMATION SECURITY
## CREDITS – 4 (LTP: 3,0,2)

**Course Objective**:
To learn information assurance techniques in area of information security.

**Teaching and Assessment Scheme:**

| Teaching Scheme (Hours per Week) | | | Credits | Assessment Scheme | | | | Total Marks |
|---|---|---|---|---|---|---|---|---|
| | | | | Theory Marks | | Practical Marks | | |
| L | T | P | C | ESE | CE | ESE | CE | |
| 3 | 0 | 2 | 4 | 60 | 40 | 20 | 30 | 150 |

**Course Contents:**

| Unit No. | Topics | Teaching Hours |
|---|---|---|
| 1 | **Conventional Encryption:** Conventional encryption model, Steganography, Classical encryption techniques: Substitution and Transposition techniques. | 3 |
| 2 | **Number Theory:** Prime and relative prime numbers, Modular arithmetic, Euler's theorem, Euclid's algorithm, Discrete logarithm tics, Modular arithmetic, The Euclidean algorithm, Finite field of the form, Extended Euclidean algorithm. | 4 |
| 3 | **Block cipher methods:** Stream ciphers and block ciphers, Block cipher structure, Data encryption standard (DES) with example, Strength of DES, Blowfish, Cast128 Design principles of block cipher, AES with structure, Traffic confidentiality, Random number generation, Key distribution. | 9 |
| 4 | **Advanced symmetric cipher:** Multiple encryption and triple DES, Electronic code book, Cipher block chaining mode, Cipher feedback mode, Output feedback mode, Counter mode. | 5 |
| 5 | **Public Key Cryptography:** Public key cryptosystems with applications, Requirements and cryptanalysis, RSA algorithm, Its computational aspects and security, Diffie-hillman key exchange algorithm, Man-in-Middle attack. | 6 |
| 6 | **Message authentication and hash functions:** Authentication requirement, Functions, Message authentication code, Hash functions, Security of hash functions and macs, MD5 message digest algorithm, Secure hash algorithm, Hmac. | 7 |
| 7 | **Network Security:** Digital signatures, Authentication protocols, Digital signature standards, Application authentication techniques like Kerberos, X.509 authentication services, Active directory service. | 6 |
| 8 | **IP Security and Web Security:** IP security overview, Architecture, Authentication header, Key management, Pretty good privacy, S/Mime and types, Web security requirement, SSL and transport layer security, Secure electronic transactions, Firewall design principles, Types of firewalls. | 5 |
| | **Total** | **45** |

**List of References:**


1. WilliamStallings, *"Cryptography and Network Principles and Practice"*,Third and Seventh Edition, Pearson Publication.
2. Faiyaz Ahamad, *"Cyber Law and Information Security"*, Dreamtech Publications.
3. Mukhopadhyay and Forouzan, *"Cryptography & Network Security"*, Third Edition, McGrawHill.
4. Atul Kahate, *"Cryptography and Network Security"*, 3rdEdition, TMH.
5. Godbole,*"Information Systems Security"*, Wiley-India
6. Deven Shah, *"Information Security Principles and Practice"*,Wiley-India


**Course Outcomes (COs):**

At the end of this course students will be able to …

1. Analyze common threats, attack and mechanism, deal with them
2. Understand and apply various Symmetric and asymmetric key Algorithms.
3. Utilize asymmetric cryptography to exchange messages.
4. Understand the concepts of Hash function, digital signature and digital certificates.
5. Apply network security with secure solution.
6. Understand professional and ethical issues with responsibilities.