**Cryptography**

**Credit 3**

**Program BE Computer Year/Semester:IV/II**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Teaching Schedule**  **Hours/Week** | | **Examination Scheme** | | | | | |
| **Theory** | **Tutorial** | **Practical** | **Internal Assessment** | | **Final** | | **Total** |
| **3** | **2** | **-** | **Theory** | **Practical\*** | **Theory\*\*** | **Practical** | **100** |
| **20** |  | **80** | **-** |

**Objective: To understand different cryptography schemes and security related issues**

1. Introduction(4H)
   1. Basic terms in cryptography
   2. Generic model of Secure Communication
   3. OSI Security Architecture
   4. Categories of Cryptographic systems
   5. Conventional Encryption Model

1. Classical Cipher Schemes(4H)
   1. Classical Substitution Ciphers: Caesar, Mono-alphabetic
   2. Hill Cipher
   3. Steganography
2. Mathematical Foundations(4H)
   1. Group, Ring, Integral Domain and Field
   2. Modular Arithmetic
   3. Residue Classes
   4. Primes and Co-Primes
   5. Euclid’s Algorithm
3. Modern Symmetric Ciphers(10H)
   1. Binary block substitution
   2. Shannon’s Theory of Diffusion and Confusion
   3. Fistel Cipher
   4. Data Encryption Standard
   5. Modes of Block/Stream Cipher
   6. International Data Encryption Algorithm (IDEA)
   7. Advances Encryption Standard (AES)
4. Public Key Cryptography(8H)
   1. Data Confidentiality using Public Key Cryptography
   2. RSA Algorithm
   3. Diffie-Hellman Algorithm for Key Distribution
5. Authentication Schemes(9H)
   1. Types of Authentication Services
   2. Techniques of Authentication
   3. Digital Signatures
   4. Message Authentication Code and Authentication
   5. Hash Function
   6. Message Digest Algorithm
   7. Secure Hash Algorithm
   8. Centralized Authentication Schemes
6. Network Security
   1. Types of Attack
   2. Security Model
   3. Email Security (PGP)
   4. Internet Protocol Security (IP Sec)
   5. Secure Socket Layer (SSL)
   6. Secure Electronic Transaction (SET)

Course References:

William Stallings: Cryptography and Network Security (Pearsons)

Kaufman: Network Security(Pearsons)

Alfred Menezes: Handbook of Applied Cryptography

Wenbo Mao: Modern Cryptography: Theory and Practice(Pearsons)

P.S. Gill: Cryptography and Network Security