Cryptography
BEG 477 CO

Year: IV **Semester:II**

Teaching Schedule Hours/Week			Examination Scheme				
Theory	**Tutorial**	**Practical**	**Internal**		**Final**		**Total**
3	**1**	**-**	**Theory**	**Practical**	**Theory**	**Practical**	**100**
			20	**-**	**80**	**-**	

Objectives: To understand differentcryptography schemes and security related issues.

1. **Introduction** **(4 hours)**
   a. Basic Terms In cryptography
   b. Generic Model of Secure Communication
   c. OSI Security Architecture
   d. Categories of Cryptographic systems
   e. Conventional Encryption model

2. **Classical Cipher schemes** **(4 hours)**
   a. Classical Substitution Ciphers : Caesar Cipher, Mono-alphabetic Cipher
   b. Hill Cipher
   c. Staganography

3. **Mathematical Foundations** **(4 hours)**
   a. Group, Ring , Integral Domain and Field
   b. Modular Arithmetic
   c. Residue Classes
   d. Primes and Co-Primes
   e. Eulicd's algorithm

4. **Modern Symmetric Ciphers** **(10 hours)**
   a. Binary Block Substitution
   b. Shannon's theory of diffusion and confusion
   c. Fistel cipher
   d. Data Encryption Standard
   e. Modes of Block / Stream Cipher
   f. International data encryption algorithm (IDEA)
   g. Advanced Encryption Standard (AES)

5. **Public-Key Cryptography** **(8 hours)**
    a. Data Confidentiality using Public-Key Cryptography
    b. RSA Algorithm
    c. Diffie-Hellman Algorithm for Key Distribution

6. **Authentication Schemes** **(9 hours)**
    a. Types of Authentication services
    b. Techniques of Authentication
    c. Digital Signatures
    d. Message Authentication Code and Authentication
    e. Hash Function
    f. Message Digest Algorithm
    g. Secure Hash Algorithm
    h. Centralized authentication Schemes

7. **Network Security** **(6 hours)**
    a. Types of Attack
    b. Security Model
    c. Email Security (PGP)
    d. Internet Protocol Security (IP Sec)
    e. Secure Socket Layer(SSL)
    f. Secure Electronic Transaction(SET)

Course References

- William Stallings : Cryptography & Network Security, 3e, Pearson Education
- Kaufamn, C., Perlman, R., &Speciner, M.,Network Security- PRIVATE Communication in Public World, Second Edition, Pearson
- Alfred Menezes : Handbook of Applied Cryptography
- Wenbo Mao : Modern Cryptography : Theory and Practice, Pearson Education
- P S Gill : Cryptography and Network Security