**KIRIROM INSTITUTE OF TECHNOLOGY**

**DEPARTMENT OF SOFTWARE ENGINEERING**

|  |  |  |  |
| --- | --- | --- | --- |
| **Instructor** | Sudhir Shenai | **Course Name** | Cryptography and Network Security |
| **Batch** | 6 | **Academic Year** | Nov 2019 - Apr 2020 |
| **Semester** | III | **Credits** | 4 |

**Course Description:**

This course is offered on sophomore year of software engineering program. The course introduces the security trends in computer networks, types of attacks, threats and defense. The major cryptography techniques, symmetric key and public key cryptography are dealt in detail. It examines the use of cryptographic and security protocols to provide security over networks and the internet. The fundamental system security threats like intruders, virus and worms are discussed in brief.

**Prerequisite:**

Should have fundamental knowledge on

* + - 1. Computer system, network and web functionalities.
      2. Network protocols specifically TCP/IP
      3. Number theory

**Learning Outcomes:**

After the completion of the course, the students will have

1. Knowledge on security trends, attacks, threats on computer networks and its counter measures.
2. Ability to identify the suitable crypto graphic techniques for security mechanisms such as authentication, confidentiality and integrity.
3. Ability to apply symmetric ciphers, public-key cryptography and hash functions for encryption and decryption.
4. Knowledge on key management principles.
5. Understanding on the functionalities of network security protocols such as SSL, TLS, Kerberos, PGP.
6. Knowledge on security facilities to protect computer systems against threats like intruders, virus and worms.

**Course Content:**

**Unit – I Introduction to Security and Cryptography**

Security Trends, OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, Model for Network security; Cryptography, Cryptosystems, Cryptanalysis; Classical Encryption Techniques -Substitution, Transposition, Steganography

**Unit – II Symmetric Ciphers**

Symmetric Cipher Model; Block Ciphers -DES, AES, Modes of Operation; Stream Ciphers and RC4; Key Distribution; Random Number – PRN Generator; Confidentiality using symmetric encryption

**Unit – III Public Key Cryptography and Hash Functions**

Principles of Public-Key Cryptosystems, RSA algorithm; Key Management - Diffie-Hellman Key Exchange; Message Authentication -MAC, Hash Functions, SHA; Digital Signatures

**Unit – IV Network Security**

Authentication – Kerberos, X.509; E-Mail Security -PGP, S/MIME; IP Security – overview, architecture; Web Security- SSL, TLS, SET

**Unit – V System Security**

Intruders -intrusion detection- password management; Malicious Software -virus and related threats -virus countermeasures; Firewalls- firewall design principles – trusted systems; Case Studies – real time incidents on security breach and recovery.

**Reference Book:**

1. William Stallings, “Cryptography & Network Security: Principles and Practice”, 4th Edition, Prentice Hall, 2005.