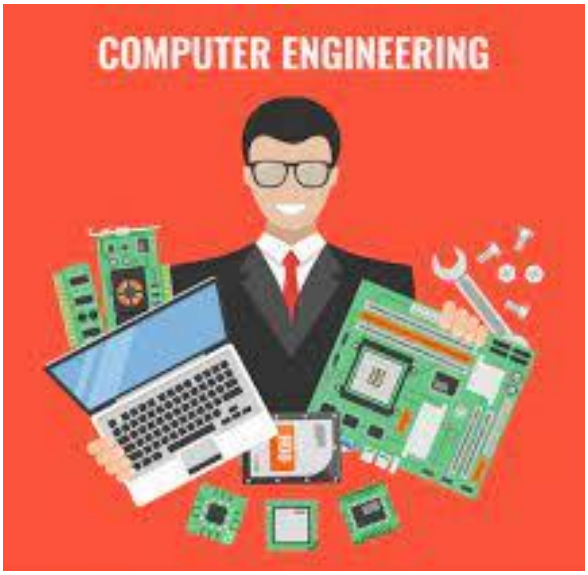
Website: www.positivequadrant.in
Email: positivequadrants@gmail.com
Contact: +91 8169150592



COMPUTER ENGINEERING

SEM VI

CRYPTOGRAPHY & SYSTEM SECURITY

Programming & development

Course Curriculum

Website: www.positivequadrant.in
Email: positivequadrants@gmail.com
Contact: +91 8169150592

CRYPTOGRAPHY & SYSTEM SECURITY SEM VI

Module 1 : Introduction to Number Theory and Basic Cryptography

- Security Goals
- Attacks
- Services and Mechanisms
- Techniques
- Modular Arithmetic
  - Euclidean Algorithm
  - Fermat's and Euler's theorem
- Classical Encryption techniques
- Symmetric cipher model
- Mono-alphabetic and polyalphabetic substitution techniques
  - Vigenere cipher
  - Playfair cipher
  - Hill cipher
- Transposition techniques
  - Keyed and keyless transposition ciphers

Module 2: Symmetric and Asymmetric key Cryptography and key Management

- Block cipher principles
- Block cipher modes of operations
- DES
- Double DES
- Triple DES
- Advanced Encryption Standard (AES)
- Stream Ciphers
  - RC4 algorithm
- Public key cryptography
  - Principles of public key cryptosystems
  - The RSA Cryptosystem
  - The knapsack cryptosystem
- Symmetric key Distribution
  - KDC
  - Needham-Schroeder protocol

Website: www.positivequadrant.in
Email: positivequadrants@gmail.com
Contact: +91 8169150592

- Kerberos
  - Kerberos Authentication protocol
  - Symmetric key agreement
  - Diffie Hellman
- Public key Distribution
  - Digital Certificate
    - X.509
    - PKI

Module 3: Cryptographic Hash Functions

- Cryptographic hash functions
- Properties of secure hash function
- MD5
- SHA-1
- MAC
- HMAC
- CMAC

Module 4: Authentication Protocols and Digital Signature Schemes

- User Authentication
- Entity Authentication
  - Password Base
  - Challenge Response Based
- Digital Signature
- Attacks on Digital Signature
- Digital Signature Scheme
  - RSA

Module 5: Network Security and Application

- Network security basics
  - TCP/IP vulnerabilities (Layer wise)
- Network Attacks
  - Packet Sniffing
  - ARP spoofing
  - Port scanning

Website: www.positivequadrant.in
Email: positivequadrants@gmail.com
Contact: +91 8169150592

  - IP spoofing
- Denial of service
  - DOS attacks
  - ICMP flood
  - SYN flood
  - UDP flood
  - Distributed Denial of Service
- Internet Security protocols
  - PGP
  - SSL
  - IPSEC
- Network Security
  - IDS
  - Firewalls

Module 6: System Security

- Buffer overflow
- Malicious programs
  - Worms and Viruses
  - SQL injection