| CSE11137 | Network Security | L | T | P | C |
|---|---|---|---|---|---|
| Version 1.0 | Contact Hours 45 | 3 | 0 | 0 | 3 |
| Pre-requisite/Exposure | Computer Network | | | | |
| Co-requisite | NIL | | | | |

**Course Objectives:**

- The course content should be taught and implemented with the aim to develop different types of skills so that students are able to acquire following competencies:
- Determine appropriate mechanisms for protecting networked systems by applying various cryptographictechniques.
- Secure the network by using firewalls on various networks in order to identify various network attacks andresolve them.

**Course Outcomes:**

On the completion of this course the student will be able to

**CO1:** Identify and describe the common types of security threats are risks to the Computer Systems and the natureof common Information hazards.

**CO2:** Identify the potential threats to confidentiality, integrity and availability of Computer Systems.

**CO3:** Describe the working of standard security mechanisms and applied to the external and internal network.

**CO4:** Define cryptography, describe the elements of the encryption process and select best algorithm to encryptdata and protocols to achieve Computer Security.

**CO5:** Apply concepts of Public Key Cryptography.

**Course Description:**

Present computing era is based on internet and hence networking is an essential part of course. Prime concern is that incurrent advanced digital world various security threats are increasing day by day posing problems to data confidentiality, integrity and availability. This course aims at learning basic cryptography techniques and applying security mechanismsfor operating systems as well as private and public network to protect them from various threats.

**Course Content:**

| Units | Lecture Hours |
|---|---|
| **Unit-I:** Introduction and Security Threats: Threats to security : Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare; Avenues of Attack, steps in attack; Security Basics | 09 |

| Units | Lecture Hours |
|---|---|
| confidentiality,Integrity, Availability; Types of attack: Denial of service (DOS), backdoors and trapdoors, Sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, Phishing attacks, Distributed DOS, SQL Injection.Malware : Viruses, Logic bombs | |
| **Unit-II:** Organizational Security: Password selection, Piggybacking, Shoulder surfing, Dumpster diving, Installing unauthorized software /hardware, Access by non-employees; People as Security Tool: Security awareness, and Individual user responsibilities; Physical security: Access controls Biometrics: finger prints, hand prints, Retina, Patterns, voice patterns, signature and writing patterns, keystrokes, Physical barriers; Password Management, vulnerability of password, password protection, password selection strategies, components of a goodpassword. | **09** |
| **Unit-III:** Cryptography and Public key Infrastructure: Introduction to Symmetric encryption & Asymmetric encryption; cipher, Vigenere cipher, one time pad (vermin cipher), hill cipher; Transposition techniques (rail fence),steganography; Hashing function : SHA1; Asymmetric encryption: Digital Signatures, Key escrow; Public key infrastructures : basics, digital signatures, digital certificates, certificate authorities, registration authorities, steps for obtaining a digital certificate, steps for verifying authenticity and integrity of a certificate; Centralized or decentralized infrastructure, private key protection; Trust Models: Hierarchical, peer to peer, hybrid. | **09** |
| **Unit-IV:** Network security: Firewalls: working, design principles, trusted systems, Kerberos; Security topologies security zones, DMZ, Internet, Intranet, VLAN, security implication, tunnelling; IP security: overview, architecture, IPSec configurations, IPSec security; Email security: security of email transmission, malicious code, spam, mail encryption. Web Security: Intruders, Intrusion detection systems (IDS): host based IDS, network based IDS, logical components of IDS, signature based IDS, anomaly based IDS, network IDS components, advantages and disadvantages of NIDS, host based IDS components, advantages and disadvantages of HIDS; Web security threats, web traffic security approaches, Introduction to Secure Socket Layer (SSL) & Transport Layer Security (TLS), Concepts of secure electronic transaction. | **09** |
| **Unit-V:** Case Study on Public Key Cryptography: Diffie Hellman key exchange protocol, Elliptic-curve cryptography, Paillier cryptosystem, Cramer Shoup cryptosystem, McEliece cryptosystem, Merkle Hellman knapsack cryptosystem. | **09** |

**Examination Scheme:**

| Components | Mid Term | Class Assessment | End Term |
|---|---|---|---|
| Weightage (%) | 20 | 30 | 50 |

## Relationship between Course Outcomes (COs) and Program Outcomes (POs):

1 = Weakly Mapped

2 = Moderately Mapped3 = Strongly Mapped

| Course Code | Course Name | COs | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 | PO 8 | PO 9 | PO 10 | PO 11 | PO 12 | PSO1 | PSO2 | PSO3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CSE111 | Netwo | CO1113 | 3 | 2 | 2 | 2 | 1 | 3 | 2 | - | 3 | - | - | 2 | 2 | 3 | 3 |
| 37 | rk | 7.1 | | | | | | | | | | | | | | | |
| | Securi ty | CO1113 7.2 | 3 | 2 | 3 | 3 | 2 | 3 | 1 | - | 3 | - | - | 2 | 2 | 2 | 2 |
| | | CO1113 | 3 | 1 | 2 | 1 | 3 | 3 | 1 | - | 2 | - | - | 2 | 3 | 3 | 3 |
| | | 7.3 | | | | | | | | | | | | | | | |
| | | CO1113 | 2 | 2 | 3 | 3 | 3 | 1 | 2 | - | 1 | - | - | 3 | 1 | 3 | 3 |
| | | 7.4 | | | | | | | | | | | | | | | |
| | | CO1113 | 3 | 2 | 3 | 3 | 2 | 1 | 3 | - | 3 | - | - | 2 | 2 | 1 | 2 |
| | | 7.5 | | | | | | | | | | | | | | | |
| | | CO1113 | 2. | 1. | 2. | 2. | 2. | 2. | 1. | - | 2. | - | - | 2.2 | 2.0 | 2.4 | 2.6 |
| | | 7 | 8 | 8 | 6 | 4 | 2 | 2 | 8 | | 4 | | | | | | |