**FR. Conceicao Rodrigues College Of Engineering**

Father Agnel Ashram, Bandstand, Bandra-west, Mumbai-50

**Department of Information Technology**

**T.E. (IT) (semester V)  (2019-2020)**

**Lesson Plan**

**Subject: Cryptography and Network Security (CNS)** **Course ID: ITC504**

**Credits-4**

SYLLABUS

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr.**  **No.** | **Module** | **Detailed Content** | **CO**  **Mapping** |
| 00 | Prerequisite | Basic concepts of OSI Layer 02 | ------- |
| 01 | Introduction & Number  Theory | Services, Mechanisms and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, mono-alphabetic and poly-alphabetic substitution techniques: Vignere cipher, playfair cipher, Hill cipher,  transposition techniques: keyed and keyless transposition ciphers, steganography). | CO1 |
| 02 | Block Ciphers &  Public Key  Cryptography | Data Encryption Standard-Block cipher  principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm.  Public key cryptography: Principles of public key cryptosystems-The RSA algorithm, The knapsack algorithm, El-Gamal Algorithm.  Key management – Diffie Hellman Key  exchange | CO1,CO2 |
| 03 | Cryptographic Hashes,  Message Digests and  Digital Certificates | Authentication requirement – Authentication  function , Types of Authentication, MAC – Hash function – Security of hash function and MAC –MD5 – SHA – HMAC – CMAC,  Digital Certificate: X.509, PKI | CO3 |
| 04 | Digital signature  schemes and  authentication Protocols | Digital signature and authentication protocols  : Needham Schroeder Authentication  protocol, Digital Signature Schemes – RSA,EI Gamal and Schnorr, DSS | CO3 |
| 05 | Network  Security | Network security basics: TCP/IP  vulnerabilities (Layer wise), Packet Sniffing, ARP spoofing, port scanning, IP spoofing,TCP syn flood, DNS Spoofing. Denial of Service: Classic DOS attacks, Source Address spoofing, ICMP flood, SYN flood, UDP flood, Distributed Denial of Service, Defenses against Denial of Service Attacks.  Firewalls, Intrusion Detection Systems: Host Based and Network Based IDS, Honey pots | CO4 |
| 06 | Network  Security  Applications | Authentication Applications, Kerberos,  Internet Security Protocols: SSL, TLS,  IPSEC:AH, ESP, Secure Email: PGP and S/MIME, Key Management | CO5 |

**Internal Assessment for 20 marks:**

Consisting of **Two Compulsory Class Tests**

Approximately 40% to 50% of syllabus content must be covered in First test and remaining 40% to

50% of syllabus contents must be covered in second test

**Course Outcome statements:**

|  |  |
| --- | --- |
| Sr.No. | Course Outcome Statement |
| ITC504.1 | Implement symmetric and asymmetric key cryptographic algorithms. |
| ITC504.2 | Compare and implement appropriate cryptographic techniques for authentication and confidentiality. |
| ITC504.3 | Evaluate the performance of hashing algorithms. |
| ITC504.4 | Identify types of attacks and evaluate performance of firewall and Intrusion Detection system using open source technology |
| ITC504.5 | Apply knowledge of security mechanisms to design secure application |

**CO-PO-PSO Mapping**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Course Name** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** | **PO11** | **PO12** | **PSO1** | **PSO2** |
| ITC504.1 | 3 |  | 2 |  |  |  |  |  |  |  |  |  |  |  |
| ITC504.2 | 3 | 2 | 2 |  | 2 |  |  |  |  |  |  |  |  | 2 |
| ITC504.3 | 3 | 2 |  | 2 |  |  |  |  |  |  |  |  |  |  |
| ITC504.4 | 1 | 2 | 2 |  | 3 |  |  |  |  |  |  |  | 2 | 2 |
| ITC504.5 | 3 |  | 3 |  | 3 | 2 | 1 | 2 |  |  |  |  | 2 | 2 |

**CO Assessment Tools**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CO number** |  | | |  | | **Indirect Measures** | |
|  | **UT1** | **UT2** | **Assignments** | | **LAB** | | **Presentations/Projects** | | **Univ. Theory** | **Course Exit Survey** |
| ITC504.1 | 20 |  | 30 | | 20 | | 20 | | 20 | 100 |
| ITC504.2 | 20 |  | 30 | | 20 | | 20 | | 20 | 100 |
| ITC504.3 |  | 20 | 30 | | 10 | | 20 | | 20 | 100 |
| ITC504.4 |  | 30 | 20 | | 20 | | 10 | | 20 | 100 |
| ITC504.5 |  | 20 | 20 | | 20 | | 20 | | 20 | 100 |

**Curriculum Gap/ NILL**

**Content beyond syllabus**

**Lecture Plan:**

| No of classes available: | 46 | No of Classes taken: | 45 |
| --- | --- | --- | --- |
|  |  |  |  |  | |
| **Sr. No. and name** | **Topic Planned** | **Planned Date** | **Actual Date** | | **Delivery Mechanisms** |
| **0** | Basic Concepts of OSI layer | 2/7/2019 | 2/7/2019 | | Chalk and Board, PPT |
| **1.**  **Introduction to number Theory** | Services, Mechanisms -attacks | 3/7 | 3/7 | | Chalk and Board,PPT |
| Attacks OSI security architecture Network security model | 4/7 | 4/7 | |
| Network security model | 5/7 | 5/7 | |
| Classical Encryption techniques Symmetric cipher model, mono alphabetic | 9/7 | 9/7 | |
| polyalphabetic substitution techniques:  Vignere cipher, playfair cipher, | 10/7 | 10/7 | |
| Hill cipher | 11/7 | 11/7 | |
| transposition techniques: keyed and keyless  transposition ciphers, | 12/7 | 12/7 | |
| steganography | 16/7 | 16/7 | |
| **2 .**  **Block Ciphers and Public Key Cryptography:** | Block Ciphers and Public Key Cryptography:  DES- block cipher principles, modes of operations. | 17/7 | 17/7 | | Chalk and Board,PPT |
| DES | 18/7 | 19/7(lecture taken by JR) | |
| AES | 19/7 | 23/7 | |
| Triple DES- Blowfish | 23/7 | 24/7 | |
| - RC5 algorithm | 24/7 | 25/7 | |
| Public key cryptography: Principles of public key cryptosystems- RSA algo, | 25/7 | 26/7 | |
| Knapsack algo | 26/7 | 30/7 | |
| El-Gamal Algo | 30/7 | 31/7 | |
| Key management – Diffie Hellman Key exchange | 31/7 | 1/8 | |
| **3.**  **Cryptographic Hashes, Message Digest and Digital Certificates** | Authentication requirement- Authentication function, Types of authentications, | 1/8 | 2/8 | | Chalk and Board,PPT |
| Types of authentications | 2/8 | 6/8 | |
| MAC-Hash function- Security of Hash function | 6/8 | 7/8 | |
| MAC- MD5 | 7/8 | 9/8 | |
| SHA- HMAC | 8/8 | 20/8 | |
| CMAC | 9/8 | 21/8 | |
| Digital Certificate: X.509,PKI | 20/8 | 22/8 | |
| **4.**  **Digital Signature schemes and authentication protocols:** | Digital Signature and authentication protocols: Needham Schroeder Authentication protocol | 21/8 | 23/8 | | Chalk and Board,PPT |
| Digital Signatures Schemes- RSA | 22/8 | 26/8 | |
| EI Gamal | 27/8 | 28/8 | |
| Shnorr | 28/8 | 29/8 | |
| DSS | 29/8 | 11/9 | |
| **5.**  **Network Security** | TCPIP vulnerabilities (layerwise), packet sniffing,ARP spoofing Distributed DOS, Defenses against DOS attacks. | 30/8 | 13/9 | | Chalk and Board,PPT |
| IP spoofing, TCP syn flood, DNS spoofing | 11/9 | 17/9 | |
| DOS- classic attacks, | 17/9 | 18/9 | |
| source address spoofing, ICMP flood, SYN flood, UDP flood, | 18/9 | 20/9 | |
| Distributed DOS, Defenses against DOS attacks | 19/9 | 24/9 | |
| Firewalls | 20/9 | 25/9 | |
| Intrusion detection system | 24/9 | 25/9 | |
| **6.**  **Network Security applications: -** | Authentication applications | 25/9 | 26/9 | | Chalk and Board,PPT |
| Kerberos, | 26/9 | 27/9 | |
| Security protocols: SSL, TLS. | 3/10 | 3/10 | |
| IPSEC: AH, ESP, | 4/10 | 9/10 | |
| secure email: PGP | 5/10 | 10/10 | |
| S/MIME, key Management | 9/10 | 10/10 | |
| Revison | 11/10 | 11/10 | | Chalk and Board,PPT |

**Lab Plan for Software Development Lab**

**Lab Outcomes:**

Students will learn to:

1. Apply the knowledge of symmetric cryptography to implement simple ciphers

2. Analyze and implement public key algorithms like RSA and El Gamal

3. Analyze and evaluate performance of hashing algorithms

4. Explore the different network reconnaissance tools to gather information about networks

5. Use tools like sniffers, port scanners and other related tools for analyzing packets in a network.

6. Apply and set up firewalls and intrusion detection systems using open source technologies and

to explore email security.

Lab Plan: CNS

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No | Topic | Week No | Lab outcome |
| 1 | Design and Implementation of a product cipher | Week1 | LO1 |
| 2 | Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA/El Gamal | Week2 | LO2 |
| 3 | Implementation of Diffie Hellman Key  exchange algorithm | Week3 | LO2 |
| 4 | For varying message sizes, test integrity of  message using MD-5, SHA-1, and analyse the performance of the two protocols. Use crypt  APIs | Week 4 | LO3 |
| 5 | Exploring wireless security tools like Kismet, NetStumbler etc. | Week5 | LO2,LO3 |
| 6 | IPTABLES | Week6 | LO6 |
| 7 | Study of packet sniffer tools wireshark, | Week7 | LO4,LO5 |
| 8 | Download and install nmap | Week8 | LO5 |
| 9 | Detect ARP spoofing using nmap and/or open source tool ARPWATCH and wireshark. | Week9 | LO4,LO5 |
| 10 | Simulate DOS attack using Hping and other tools. | Week9 | LO4,LO5 |
| 11 | Explore the GPG tool of linux to implement email security. | Week10 | LO6 |

**Assignment Plan:**

|  |  |  |
| --- | --- | --- |
| **Assignment No** | **Date** | **CO/LO** |
| **1** | **15/09/2019** | **CO1,CO2** |
| **2** | **1/10/2019** | **CO3,CO4,CO5** |

**Term Work:**

Term Work shall consist of at least 10 to 12 practical’s based on the above list. Also Term work

Journal must include at least 2 assignments.

**Term Work Marks:** 25 Marks (Total marks) = 15 Marks (Experiment) + 5 Marks (Assignments) + 5

Marks (Attendance)

**Oral Exam:** An Oral exam will be held based on the above syllabus.