**Lab Plan**

**Name of the Course:** Cryptography and System Security

**Year/Sem/Class:** AI and DS / Sem VI / D11AD

**Prerequisite:** Operating System, Basics of Java and Python Programming.

**Lab Objectives:**

1 To be able to apply the knowledge of symmetric cryptography to implement simple ciphers

2 To be able to analyze and implement public key algorithms like RSA and El Gamal

3 To analyze and evaluate the performance of hashing algorithms

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

**Lab Outcomes:**

1\* Design and Implementation of a product cipher using Substitution and Transposition ciphers.

2\* Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA/El Gamal.

3\* Implementation of Diffie Hellman Key exchange algorithm

4 For varying message sizes, test the integrity of the message using MD-5, SHA-1, and analyze the performance of the two protocols. Use crypt APIs.

5\* Exploring wireless security tools like Kismet, NetStumbler etc.

**Index**

| **Exp. No.** | **Lab Experiments** | **CO** | **DOP** | **DOS** | **Marks** | **SIGN.** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Design and Implementation of a product cipher using Substitution and Transposition ciphers. | CO1 |  |  |  |  |
| 2 | Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA/El Gamal. | CO1 |  |  |  |  |
| 3 | Implementation of Diffie Hellman Key exchange algorithm | CO1, CO2 |  |  |  |  |
| 4 | For varying message sizes, test the integrity of messages using MD-5, and SHA-1, and analyze the performance of the two protocols. Use crypt APIs. | CO2, CO3 |  |  |  |  |
| 5 | Exploring wireless security tools like Kismet, NetStumbler etc. | CO2, CO3 |  |  |  |  |
| 6 | Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars. | CO2, CO3, CO4 |  |  |  |  |
| 7 | Study of packet sniffer tools Wireshark,:- 1. Observer performance in promiscuous as well as non-promiscuous mode. 2. Show the packets can be traced based on different filters. | CO2, CO5 |  |  |  |  |
| 8 | Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc. . | CO1, CO3, C05 |  |  |  |  |
| 9 | Detect ARP spoofing using Nmap and/or open-source tool ARPWATCH and Wireshark | CO3, CO5 |  |  |  |  |
| 10 | Use the NESSUS/ISO Kaali Linux tool to scan the network for vulnerabilities | CO5, CO6 |  |  |  |  |

**Grading for Credit Based Grading System (CBSGS)**

| **Sr. No.** | **Range** | **Grade** | **Grade Point** |
| --- | --- | --- | --- |
| **1** | **80 and above** | **Outstanding (O)** | **10** |
| **2** | **75.00 – 79.99** | **Excellent (A)** | **9** |
| **3** | **70.00 – 74.99** | **Very Good (B)** | **8** |
| **4** | **60.00 – 69.99** | **Good (C)** | **7** |
| **5** | **50.00 – 59.99** | **Fair (D)** | **6** |
| **6** | **45.00 – 49.99** | **Average (E)** | **5** |
| **7** | **40.00 – 44.99** | **Pass (P)** | **4** |
| **8** | **Less than 40.00** | **Fail (F)** | **0** |

**Name Of Lab Teacher: Name of Subject Teacher:**

**Signature Signature:**