**THADOMAL SHAHANI ENGINEERING COLLEGE**

**Department of Computer Engineering**

**Academic Year 2021 – 22**

**T. E. Computer Semester: VI**

**List of Experiments**

**Subject: Cryptography and System Security Lab. (CSS Lab.)**

|  |  |
| --- | --- |
| **S. No.** | **Name of Experiments** |
|  | Implementation of Caesar Cipher |
|  | Implementation of Playfair Cipher |
|  | Implementation of Extended Euclidean algorithm |
|  | Implementation of Euler’s Totient Function |
|  | Implementation of RSA cryptosystem |
|  | Implementation of Diffie Hellman Key exchange algorithm |
|  | Study the use of network reconnaissance tools and apply the following: WHOIS, dig, traceroute, nslookup. |
|  | Study and implementation of packet sniffer tool: wireshark |
|  | Design of personal Firewall using Iptables |
|  | Simulation of Buffer Overflow Attack |
|  | Simulation of SQL Injection Attack [Optional] |
|  | Simulation of port scanning attack using Nmap [Optional] |

Subject In-charge

Ms. Nabanita Mandal

**THADOMAL SHAHANI ENGINEERING COLLEGE**

**Department of Computer Engineering**

**Academic Year 2021 – 22**

**T. E. Computer Semester: VI**

**Assignment**

1. Why digital signatures are and digital certificates are required?

2. List software vulnerabilities. How are they exploited to launch an attack?