**SIR PADAMPAT SINGHANIA UNIVERSITY, UDAIPUR**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**B.Tech**

**Experiment List**

**Lab Name:** Fundamentals of Cryptography Lab **Lab code:** CSE2336

**Branch:** CSE (Cyber Security ) **Sem:**3rd Sem

1. **Write a C program that contains a string (charpointer) witha value\Hello World’.The program should XOR each character in this string with 0 and display the result.**
2. **Write a C program that contains a string (char pointer) with a value \Hello World’. The program should AND and XOR each character in this string with 127 and 255 respectively display the result.**
3. **Write a program in C to implement Caeser Cipher.**
4. **Write a program in C to implement Monoalphabetic substitution cipher**
5. **Write a program in C to implement Vigenere (Polyalphabetic) Cipher**
6. **Study of Packet Sniffer Tools: Wireshark**
7. **Download and install wireshark and capture icmp, tcp and http packets in promiscuous mode.**
8. **Explore how the packets can be traced based on different filters.**
9. **Study the Use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registers.**
10. **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.**
11. **Implementation and analysis of RSA cryptosystem and RSA/ElGamel.**
12. **Implementation of Diffie/Hellman Key exchange algorithm.**
13. **For varying message sizes, test integrity of message using MD-5, SHA-1, and analyse the performance of two protocols. Use Crypt API**
14. **Detect ARP spoofing using nmap and/or open-source tool ARPWATCH and Wireshark. Use arping tool to generate gratuitous arps and monitor using Wireshark.**
15. **Simulate DOS attack using Hping, hping3 and other tools.**
16. **Simulate buffer overflow attack using Ollydbg, Splint, Cppcheck etc.**
17. **Setup IPSEC under Linux. Setup snort and study the logs.**
18. **Setting up personal firewall using iptables.**
19. **Explore the GPG tool of linux to implement email security.**
20. **SQL injection attack , Cross-Cite Scripting attack simulation.**