



**K J Somaiya College of Engineering**

**Department of Computer Engineering**

List of Experiments - Post Lab Questions

**Course: Information Security (116U01L602)**

Semester: VI Year: 2022-2023 (Second Term)

|  |  |
| --- | --- |
| **Course Outcome** | After completion of this course students should be able to |
| **CO1** | Explain various security goals, threats, vulnerabilities and controls |
| **CO2** | Apply various cryptographic algorithms for software security |
| **CO3** | Identify and analyse web attacks |
| **CO4** | Illustrate and Compare network security mechanisms |
| **CO5** | Interpret legal and ethical issues in security |

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Topic** | **CO Mapping** |
| 1 | Encryption-Decryption programs using classical cryptography | CO1,CO2 |
| 1.1 Write the points of difference between mono-alphabetic cipher and poly-alphabetic cipher. |
| 1.2 Explain the working of a rail-fence cipher with the help of an example. |
| 1.3 Discuss any three applications of cryptography. |
| 2 | Application of RSA Algorithm for various security services like confidentiality, authentication, signature, non-repudiation and integrity | CO1,CO2 |
| 2.1 In the RSA algorithm, p= 7, q=11 and e= 13, then what will be the value of d? |
| 2.2 Discuss various cryptanalysis attacks possible to be carried out on RSA |
| 2.3 Comment on drawbacks of RSA. Discuss solution(s) over the same. |
| 3 | Non-malicious program flaws - Buffer Overflow and its prevention | CO2 |
| 3.1 What is the difference between malicious and non-malicious program flaws? Give suitable examples of each. |
| 3.2 Explain different types of buffer overflow attack. |
| 3.3 List the mechanisms to prevent buffer overflow attack. |
| 3.4 How canary values are used to overcome stack buffer overflow? |
| 4 | Analysis of sample vulnerable web applications for Man-in-Middle Attack / SQL injection etc. using Burp Suite.  4.1 Which are the major types of web application attacks?  4.2 How to mitigate the SQL Injection attacks?  4.3 Explain man in middle attack. | CO3 |
| 5 | Introduction to Open Web Application Security Project and implementation of XSS.  5.1 What is OWASP? List the latest web security application risks by OWASP.  5.2 Explain countermeasures for injection attacks.  5.3 List the types of XSS attacks. | CO3 |
| 6 | Email security using PGP implementation (Pretty Good Privacy). | CO4 |
| 6.1 In PGP, explain how Bob and Alice exchange the secret key for encrypting the messages? |  |
| 6.2 List the types of algorithms used in PGP. |  |
| 6.3 Explain the significance of key rings in PGP. |  |
|  | 6.4 Distinguish between PGP and S/MIME. |  |
| 7 | Implementation and configuration of Firewall using Iptable / Fortinet / Palo Alto.  7.1 What is the difference between stateful and stateless firewalls?  7.2 How does a firewall protect data?  7.3 What can't a firewall protect against?  7.4 How is a firewall different from an IDS and an IPS? Explain. | CO4 |
| 8 | Working with sample real life cases related to Network security and forensics using tools like NMAP and Network Miner. | CO4 |
| 8.1 Explain the different challenges in handling network based incidents. |
| 8.2 Discuss the tools used for monitoring the network traffic. |
| 8.3 What do you understand by packet sniffing? |
| 9 | Implementation of CAPTCHA for Security of systems | CO4 |
| 9.1 Discuss how CAPTCHA helps in improving web security. |
| 9.2 What are the different types of CAPTCHA? Is re-CAPTCHA different from CAPTCHA? Justify your answer. |
| 9.3 List the limitations of CAPTCHA. Mention the alternatives to CAPTCHA which can overcome these limitations. |
| 10 | Report writing on legal issues and ethics with respect to some case study. | CO5 |
| **Virtual Lab Experiments - vlab.co.in** | | |
| 1 | Encryption Decryptions  Virtual Laboratory Experiments- (<http://cse29-iiith.vlabs.ac.in/>)   1. [Breaking the Shift Cipher](http://cse29-iiith.virtual-labs.ac.in/exp1/index.php) b. Breaking the Mono-alphabetic Substitution Cipher | CO2 |
| 2 | Public-Key Cryptosystems (PKCSv1.5) | CO2 |
|  | **Challenge Experiment** |  |
|  | Explore Kali Linux Security and Forensics Tools | CO3,CO4 |

* Students can perform experiments of their choice other than this list with prior permission
* Students are also required to execute programs on IIT Virtual Laboratory

**16 Jan 2023**

**Course Teachers**