Charotar University of Science and Technology

Devang Patel Institute of Advance Technology and Research

Department of Computer Science & Engineering

Subject: Cryptography and Network Security **Semester: 6**

Subject Code: CS345 **Academic Year: 2022-23**

Course Outcomes (COs):

CO1	Understand Symmetrical and Asymmetrical cryptography encryption techniques
CO2	Describe network security services and mechanisms
CO3	Understand Data integrity, Digital Signatures, key Management, Public-KeyInfrastructure
CO4	Evaluate the authentication and hash algorithms.
CO5	Practically work on various network security applications, IPsec, Firewall, IDS,Web security, Email security, and malicious software etc
CO6	Perform simple vulnerability assessments and password audits and also able toconfigure simple firewall architectures and Understand Virtual Private Networks

Experiment List

Sr. No.	Aim of the Practical	Hrs.	CO
1	Apply attacks for cryptanalysis to decrypt the original message from a given cipher text using Caesar-Cipher .Soldier from field wants to send message to base. Implement the cipher to decrypt message. Decrypt message :KLURVKLPD for caesar cipher.	2	1
2	Soldier from field wants to send message to base. Implement the cipher to decrypt message.Using Playfair,Decrypt the message: BWPNRSMUALAW,Use key : pearlharbour	2	1

3	The Rail Fence Cipher was invented in ancient times. It was used by the Greeks, who created a special tool, called scytale, to make message encryption and decryption easier. The letters are arranged in a way which is similar to the shape of the top edge of the rail fence. If king Leonidas want to send message to Sparta as "300 achieved glory at hot gate, unite for Greece" then what will be ciphertext when it is encrypted using 3 rows. Also implement decryption ofmessage.	2	1
4	The transmission of information needs to be secure over the communication channel and the data has to be confidential. Study and implement the practical approach for Steganography. -Using DOS commands -Using OpenPuff Tool	2	1
5	Implement GPG for windows.	2	4
6	Configure Nmap (Network mapping tool) on Linux/Windows. Explore the various command for scanning your host/ips, ports and various services running on port. Prepare the document of at least 25 Nmap commands. Use the Nmap script and launch the DoS attack by flooding the packages in regular interval.	2	1
7	Perform Port Scanning, File Transfer, Client-server chat and Basic Webserver implementation using netcat. Find the service running on the particular port using netcat.	2	1
8	Bob is going to send his encrypted file using public key shared by Alice using Public-key infrastructure. Alice will decrypt the file by using her private key and ensure the confidentiality. Implement the given scenario using RSA algorithm.	2	1
9	In computers, Foot printing is the process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment. Foot printing can reveal system vulnerabilities and improve the ease with which they can be exploited. Use the given approach to implement Footprinting: Gathering Target Information making use of following tools: • Dmitry – Deepmagic • ~~UA Tester~~ • Whatweb	2	1
10.	Find out Web Application Vulnerability using OWASP-ZAP tool.	2	2
11.	Implement hash function for the given Scenario.	2	2
12.	Implement DES/AES algorithm for the given plain text.	2	3

Prepared By: Ms. Rima Patel