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: 2021-22**

Course Outcomes (COs):

After completion of the course students will be able to:

1. Define various security goal and understand the security policies such as the CIA triad of Confidentiality, Integrity and Availability.
2. Classify various forms of security attacks, where they arise, and appropriate tools or mechanism to quantify them.
3. Illustrate a basic understanding of cryptography, how it has evolved, and evaluate symmetric key encryption techniques used today.
4. Distinguish modern symmetric encryption standard, key distribution scenario and analyze effectiveness in todays' environment.
5. Evaluate Asymmetric key encryption techniques, key distribution scenario and calculate public and private components of asymmetric key encryption techniques.
6. Develop message integrity and message authentication of message digest.

Practical List

Sr. No.	AIM	Hrs	COs
1	The "Caesar Box," or "Caesar Cipher," is one of the earliest known ciphers. Developed around 100 BC, it was used by Julius Caesar to send secret messages to his generals in the field. In the event that one of his messages got intercepted, his opponent could not read them. This obviously gave him a great strategic advantage. Caesar shifted each letter of his message few letters to the right to produce what could be called the ciphertext. The ciphertext is what the enemy would see instead of the true message. So, for example, if Caesar's messages were written in the English alphabet, and shift by 3 then each letter "A" in the message would become a "D," the "B's" would become "E's," and the "X's" become "A's." This type of cipher is appropriately called a "shift cipher." Implement the cipher in any programming language of your choice. Perform encryption, decryption. Discuss and try some possible attacks on traditional Caesar cipher.	**2**	**3, 4**
2	The Playfair cipher was predominantly used by British forces during the Second Boer War (1899-1902) and World War I (1914-1918). Soldier from field wants to send message to base. Implement the cipher to encrypt and decrypt message. Encrypt message : Hiroshima Use key : pearlharbour	**2**	**3, 4**
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 of message.	**2**	**3, 4**
4	RSA algorithm is used by Salim to transfer session key to Anarkali. He suspects that Akbar is performing man in middle attack he chose to use 1024 bit prime numbers. Hint: you may choose to use big integer in java.	**2**	**5**
5	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, 3**
6	Implement GPG for windows.	**2**	**1**
7	Perform port scanning using nmap on a single port and capture the packets using wireshark and analyze the output.	**2**	**2**
8	a. Perform Port Scanning, File Transfer, Client-server chat and Basic Webserver implementation using netcat. b. Find the service running on the particular port using netcat.	**2**	**2**
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**	**2, 3**
10	Find out Web Application Vulnerability using OWASP-ZAP tool.	**2**	**1, 2, 3**