Charotar University of Science and Technology

Devang Patel Institute of Advance Technology and Research

Department of Computer Engineering

Subject Name: Information security

Subject Code: CE348 **Academic Year: 2022-23**

Course Outcomes (COs):

CO1 Define various security goal and understand the security policies such as the CIA triad of Confidentiality, Integrity and Availability.

CO2 Classify various forms of security attacks, where they arise, and appropriate tools or mechanism to quantify them.

CO3 Illustrate a basic understanding of cryptography, how it has evolved, and evaluate symmetric key encryption techniques used today.

CO4 Distinguish modern symmetric encryption standard, key distribution scenario and analyse effectiveness in todays' environment**.**

CO5 Evaluate Asymmetric key encryption techniques, key distribution scenario, calculate public and private components of asymmetric key encryption.

CO6 Develop message integrity and message authentication of message digest.

Practical List

Sr. No.	Aim Of the Practical	Hrs.	CO
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.	02	1,2,3
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	02	1,2,3
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 sent 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.	04	1,2,3
4.	Sergio wants to pass encrypted message to Rafael. He is using Hill cipher. Message : family Key : consider 3x3 matrix Implement encryption and decryption of message.	02	1,2,5
5.	Mr. Lucious Fox wants to transfer small amount of data within one session to Bruce wayne. But they know that joker is listening/tapping to communication so they want communication to be encrypted with secret key. Implement Diffie hellman algorithm to help them establishing key for session.	04	2,3,4
6.	After establishing connection with bruce wayne , established shared secret is used as a input to a random number generator available at both ends. Generated random numbers will follow same sequence at both ends. They are used as a one time pad for encrypting/decrypting message. Message is converted to binary numbers and then encrypted with ex-or operation. Implement above system as a stream of message. Consider A=1, B=2, C=0…. So one	02	2,3,4
7.	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.	04	2,3,5

8.	Salim received some doubtful message from Anarkali. He is doubtful that messages are tempered by some attacker during transmission so he asks Anarkali to digitally sign the messages. Implement system for transferring message with non-repudiation.	02	2,3,5
9.	Viru sent important content in file along with hash of file content along with it. At the receivers end , how Raju can check integrity of file? Show that even slight in change in file content will bring significant change in hash value.	02	5,6
10.	Demonstrate working of Digital Signature using Cryptool.	04	3,5
11	Demonstrate image steganography using any programming language of your choice	02	3,4