St. Vincent Pallotti College of Engineering & Technology, Nagpur
Department of Computer Engineering
Session 2024-25
CNS Practical Details

Practical 1:

Aim: To implement Substitution Techniques

1A.

Case Study:

A popular messaging app, "Secure Chat," wants to enhance the security of its users' conversations. The app currently uses a simple encryption method, but the developers want to implement a more robust and secure approach to protect user data. The developers decided to use Caesar Cipher, Modified Caesar Cipher and Vigenere Cipher substitution techniques in cryptography to achieve this goal.

Objective:

The objective is to design and implement a simple and polyalphabetic substitution-based encryption algorithms to secure user messages in the Secure Chat app.

Requirement & Working:

Step 1: Key Generation

- √ Generate a random keyword for each user that will be used for the Vigenere Cipher.
- √ Store the keyword securely on the user's device.

Step 2: Caesar Cipher / Modified Caesar

- √ Define a shift value for the mentioned technique.
- √ Encrypt each message by shifting each letter by the fixed shift value.

Step 3: Vigenere Cipher

- √ Use the generated keyword to create a series of Caesar Ciphers with different shift values.
- √ Encrypt each message by applying the corresponding Caesar cipher for each letter, based on the keyword.

Step 4: Encryption

- √ Combine the encrypted messages from the step 2 and step 3 to create the final encrypted message.

Step 5: Decryption

- √ Use the same keyword and shift values to decrypt the message.

1B.

Case Study:

The military is planning a covert operation to gather intelligence on an enemy's stronghold. The operation requires secure communication between the command center and the field agents to exchange critical information. The enemy is known to have advanced surveillance capabilities, and any breach in communication could compromise the entire operation.

Objective:

Design & Implement the **Playfair Cipher technique** to encrypt and decrypt messages between the command center and the field agents. The technique should be resistant to cryptanalysis and interception by the enemy.

Requirement & Working:

Step 1: Key Generation

- √ The command center generates a random 5x5 matrix of letters, known as the Playfair square.
- √ This matrix is shared with the field agents through a secure channel.

Step 2: Encryption

- √ When the command center needs to send a message to the field agents, it breaks the message into pairs of letters (digraphs).

√ Each digraph is then encrypted using the Playfair square using the methods as discussed in the class.

Step 3: Decryption

√ The field agents receive the encrypted message and use the same Playfair square to decrypt it. The decryption process is the reverse of the encryption process.

{Note the following:

1. **Student need to implement the code using any programming tool.**
2. **Student need to implement Vigenère Cipher table in code.**
3. **Student need to write the practical in the following order on RHS of the page:**
   a. **Aim.**
   b. **Objective.**
   c. **Theory of each algorithm separately with diagram explanation with an example.**
   d. **Algorithm as per the lab.**
   e. **Code/Implementation separately as per the given lab.**
   f. **Result & Discussion (Min 3 outputs should be displayed & discussed separately).**
   g. **Cryptanalysis (Mentioning the advantages & disadvantages of each method separately).**
   h. **Conclusion in your words.**
   i. **Neat Flowchart should be drawn that clearly explains the flow of the code on LHS of the page.}**

Prof. Reema Roychaudhary
Practical In-charge