A Project Report

on

**The Secret Cipher Problem**

*Submitted* by

DEBASMITA MUKHERJEE [RA2211026030005]

Under the Supervision of

s

Ms. Nidhi Pandey

(Assistant Professor, Department of Computer Science and Engineering)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

FACULTY OF ENGINEERING & TECHNOLOGY

SRM INSTITUTE OF SCIENCE & TECHNOLOGY

DELHI-NCR CAMPUS, MODINAGAR

SIKRI KALAN, DELHI MEERUT ROAD,

DIST. – GHAZIABAD - 201204

Odd Semester- 2023-24

**SRM INSTITUTE OF SCIENCE TECHNOLOGY**

(Under Section 3 of UGC Act, 1956)

**BONAFIDE CERTIFICATE**

Certified that this project report titled “The secret cipher problem” is the bonafide work of “DEBASMITA MUKHERJEE [Reg No.: RA2211026030005] who carried out the project work under my supervision. Certified further, that to the best of my knowledge, the work reported here does not form any other project report or dissertation.

SIGNATURE

Dr. Akash Punhani

Head of Department

Dept. of Computer Science and Engineering

SIGNATURE

Ms. Nidhi Pandey

Assistant Professor

Dept. of Computer Science and Engineering

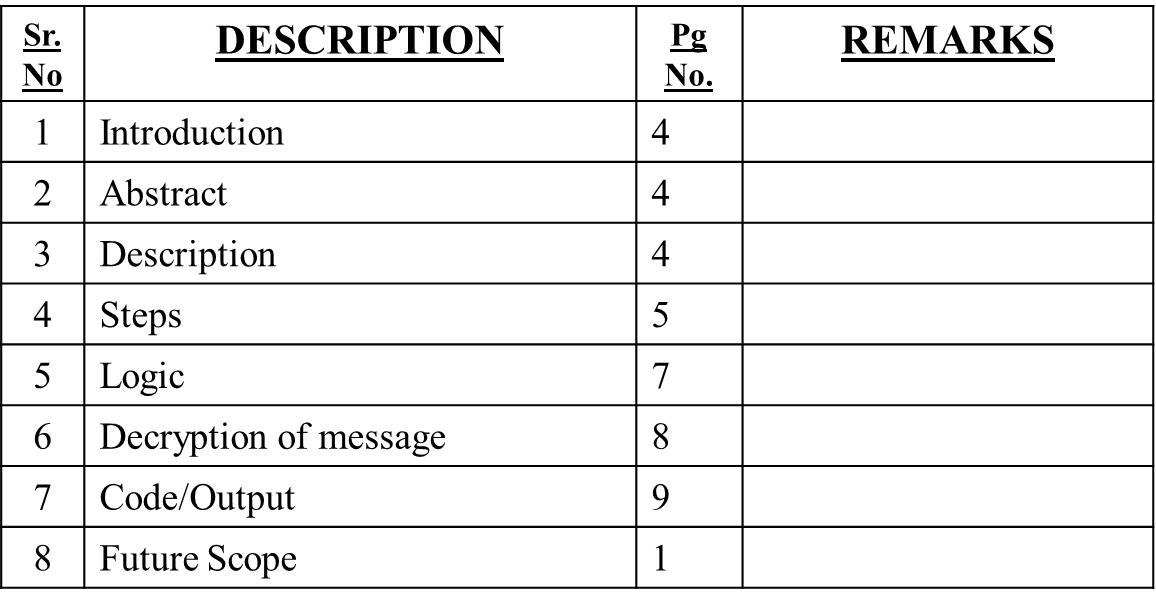
# **ACKNOWLEDGEMENTS**

We would like to thank our guide, Ms. Nidhi Pandey, for her valuable guidance, constant encouragement, personal caring, timely aid and offering timely assistance as well as providing us a wonderful environment in which to explore ourselves. Throughout the project, she has extended bright and agreeable assistance to us, despite her hectic schedule.

We would also want to express our gratitude to Dr. Akash Punhani, Professor and Head, Department of B.Tech Computer Science and Engineering, SRM Institute of Science and Technology (Delhi-NCR Campus), for his helpful recommendations and support during the project's duration. We would like to express our gratitude to the personnel and students at the SRM Institute of Science and Technology's Computer Science and Engineering Department for their assistance during our investigation. Finally, we want to express our gratitude to our parents, family, and friends for their unwavering love, constant assistance, and unwavering support.

DEBASMITA MUKHERJEE [RA2211026030005]

**Table of Contents**

****

**INTRODUCTION**

The secret cipher problem typically involves cracking an encoded or encrypted message using various cryptographic techniques. It requires deciphering a message that has been intentionally transformed using a specific cipher or encryption method. The challenge involves identifying the cipher type, recognizing patterns, using frequency analysis, and sometimes employing trial and error to decode the hidden message.

**ABSTRACT**

The secret cipher problem presents an intriguing challenge in the realm of cryptography, involving the decryption of concealed messages encoded using various cryptographic techniques. Often, it requires the application of logical deduction, pattern recognition, and encryption analysis to unveil the hidden content. Encoded messages might employ classic ciphers such as the Caesar cipher, substitution ciphers, or more sophisticated encryption methods. Solving these puzzles involves identifying the cipher type, recognizing patterns, utilizing frequency analysis, and occasionally resorting to trial and error to decipher the encrypted message, making it an engaging exercise in problem-solving within the field of codebreaking and cryptanalysis.

**DESCRIPTION**

The code provided in C attempts to decode a secret message that has been encrypted using a method called the Caesar cipher. The program tries all possible ways (or shifts) of unscrambling the message, starting from a shift of zero and going up to 25 (the total number of letters in the English alphabet). By doing this, it shows all the different versions of the message until the original, readable one is revealed. This approach allows the code to uncover the hidden message by testing each potential shift and displaying the potentially decrypted messages, one of which will be the actual message that was hidden using the Caesar cipher method.

**STEPS**

1. *Understand the Problem:* Get a clear understanding of the encrypted message and any hints or clues provided. Identify if a specific cipher or encryption method is mentioned or if you need to determine it.
2. *Identify the Cipher Type:* Try to recognize the type of cipher used. It could be a substitution cipher, Caesar cipher, Vigenère cipher, or something else. Look for patterns, clues, or any known characteristics of common ciphers.
3. *Frequency Analysis:* Analyze the frequency of letters or symbols in the encrypted text. In many languages, certain letters or characters appear more frequently than others. For example, in the word English, 'e' is the most common letter. Use this to our advantage.
4. *Trial and Error:* Apply known and basic cipher techniques. For instance, attempt to decode the message using a Caesar cipher by shifting letters in the alphabet. Try various common ciphers systematically to see if any reveal the plaintext.
5. *Pattern Recognition:* Look for recurring patterns or sequences in the encrypted message. These patterns might provide clues to decipher the message or determine the encryption method used.
6. *Known Plain Text:* If we have a section of the plaintext and its corresponding encrypted text (cipher text), use this information to deduce the pattern or key used in the encryption.
7. *Use Cryptography Tools or Resources:* Utilize online tools or software specifically designed to crack different types of ciphers. There are numerous tools available to assist in decryption if we are encountering a particularly challenging cipher.
8. *Persistence and Patience*: Solving secret ciphers can take time and may require several attempts. We need to be patient and persistent, trying different approaches or combinations until we find the right solution.
9. *Document Progress:* Keep track of the methods we have tried and any progress made. Sometimes noting down different attempts can help us avoid retracing steps or making the same mistakes.
10. *Consult and Collaborate*: If we are stuck, discussing the problem with others or seeking help from online communities interested in cryptography might provide new insights or fresh perspectives.

The complexity of the cipher and the difficulty in solving it can vary significantly. It might require a mix of logical deduction, pattern recognition, and in some cases, specialized cryptographic knowledge to decode the message.

**LOGIC**

Let’s consider a simple example using a Caesar cipher, which is a type of substitution cipher. In a Caesar cipher, each letter in the plaintext is shifted a fixed number of places down or up the alphabet.

Consider the phrase "SECRET MESSAGE" and use a basic substitution cipher, where each letter is replaced by another letter in a fixed pattern. For this example, let's create a simple substitution where each letter is shifted forward by one position in the alphabet.

1. Plain Text (Original Message):SECRET MESSAGE
2. Encryption with a Simple Substitution Cipher (Shift each letter forward by one):\*\*

So, "SECRET MESSAGE" becomes "TFDSFU NFTTBHF" when encrypted using a simple substitution cipher where each letter is shifted one position forward in the alphabet.

1. Decryption (Reverse the Substitution):To decrypt the message, reverse the substitution by shifting each letter back by one position in the alphabet.

Thus, "TFDSFU NFTTBHF" becomes "SECRET MESSAGE" when decrypted by shifting each letter back by one position in the alphabet, which is the reverse of the original encryption process.

**DECRYPTION**

- T becomes S

- F becomes E

- D becomes C

- S becomes R

- F becomes E

- U becomes T

- (space remains as a space)

- N becomes M

- F becomes E

- T becomes S

- T becomes S

- B becomes A

- H becomes G

- F becomes E

* S becomes T
* E becomes F
* C becomes D
* R becomes S
* E becomes F
* T becomes U
* (space remains as a space)
* M becomes N
* E becomes F
* S becomes T
* S becomes T
* A becomes B
* G becomes H
* E becomes F

**CODE**

#include <stdio.h>

#define ALPHABET 26

void encrypt(char message[], int shift) {

int i = 0;

char ch;

while (message[i]) {

ch = message[i];

if (ch >= 'A' && ch <= 'Z') {

ch = ((ch - 'A' + shift) % ALPHABET) + 'A';

} else if (ch >= 'a' && ch <= 'z') {

ch = ((ch - 'a' + shift) % ALPHABET) + 'a';

}

printf("%c", ch);

i++;

}

}

void decrypt(char encrypted\_message[], int shift) {

encrypt(encrypted\_message, ALPHABET - shift);

}

int main() {

char message[] = "SECRET MESSAGE";

int shift = 1;

// Encrypt the message

printf("Encrypted message: ");

encrypt(message, shift);

printf("\n");

// Decrypt the message

char encrypted\_message[] = "TFDSFU NFTTBHF";

printf("Decrypted message: ");

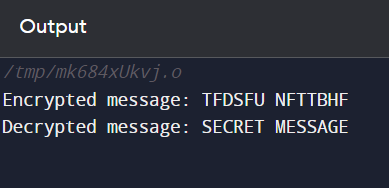
decrypt(encrypted\_message, shift);

printf("\n");

return 0;

}

**OUTPUT**



**FUTURE SCOPE**

The secret cipher problem has numerous potential future scopes and applications

1. *Post-Quantum Cryptography*: Research and development in post-quantum cryptography are essential to create encryption methods that can withstand attacks from quantum computers. Exploring new ciphers and cryptographic algorithms that are resilient against quantum attacks is a significant future scope.
2. *Cybersecurity & Privacy Enhancements*: Secret ciphers will continue to play a vital role in bolstering cybersecurity and ensuring privacy in a digital landscape. Advancements in encryption techniques will be essential for securing sensitive data, communications, and transactions.
3. *AI and Cryptanalysis*: The application of artificial intelligence and machine learning in cryptanalysis will likely evolve, aiming to break or strengthen ciphers. AI-driven approaches will help in analyzing patterns in encrypted data, potentially impacting both encryption security and decryption capabilities.
4. *Homomorphic Encryption & Secure Computation:* Future developments in privacy-preserving technologies like homomorphic encryption and secure multi-party computation will focus on enabling computations on encrypted data without revealing the data. This area holds promise for protecting sensitive information in various fields.
5. *Emerging Technologies Integration*: Integration of secret cipher techniques into emerging technologies such as the Internet of Things (IoT), blockchain, and cryptocurrencies will be pivotal for ensuring secure communications, transactions, and access control within these systems. This includes applications in device security, secure data sharing, and verification mechanisms.