Project Presentation

Substitution Techniques in Encryption - Decryption

By

MITU22BTCS0723 - Sanjyot Patil
MITU22BTCS0562 - Pranav Jagtap
MITU22BTCS0990 - Vinit Jadhav
MITU22BTCS0865 - Sujal Virkhede

Guided By

Prof. Rohidas Sangore

Department of Computer Science & Engineering, MITSOC, Loni Kalbhor

Outline

1 INTRODUCTION
2 CONCEPTS AND METHODS
3 LITERATURE SURVEY
4 PROJECT PLAN
5. SOFTWARE REQUIREMENT SPECIFICATION
6 RESULTS
7 SOFTWARE TESTING
8 CONCLUSION AND FUTURE WORK
BIBLIOGRAPHY
ANNEXURE A: List of Publications and Research Paper (In its Original formats)
ANNEXURE B: Plagiarism Report

1. Introduction

Substitution techniques are one of the oldest and simplest forms of encryption. They have been used for centuries to protect sensitive information, such as military secrets and diplomatic messages. Today, substitution techniques are still used in some **encryption algorithms**, but they are typically combined with other cryptographic techniques, such as transposition ciphers and block ciphers, to create more secure encryption systems.

2. Problem Statement

The problem statement for "**Substitution Techniques in Encryption-Decryption**" addresses issues related to the **security vulnerabilities** of these techniques, their practical applicability, their value in education, potential integration into modern cryptography, balancing historical significance, and exploring possibilities for enhancing their security. It questions their role in contemporary cryptography and the need to address their limitations and potential improvements

3. Objectives

- **Protect** the confidentiality of data
- Protecting sensitive data from unauthorized access
- To **encrypt and decrypt** data stored on computers and other devices.
- To protect data transmitted over networks.
- To create **digital signatures** for data.
- Ensure the integrity and **authenticity of data**.

4. Concepts and Methods

Substitution techniques in encryption and decryption are based on the concept of **replacing characters** or groups of characters in a plaintext message with other characters or groups of characters according to a predefined key. **The key** is a **secret piece** of information that both the sender and receiver of the message must know in order to encrypt and decrypt the message, respectively.

- Atbash Cipher
- Caesar Cipher
- Vigenère Cipher
- Substitution Table
- ROT13 Cipher

5. Literature Survey

Claude E. Shannon's work is considered one of the foundational pieces of modern cryptography. In this paper, Shannon introduced a rigorous mathematical approach to evaluate the strength and security of substitution ciphers. Shannon's work laid the foundation for assessing the **security of cryptographic systems** and contributed to the development of modern cryptography. His insights continue to be relevant and influential in the design and analysis of encryption techniques.

Simon Singh's book, "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography," provides a historical review of substitution ciphers as part of the broader exploration of the history of cryptography. In this book, Singh delves into the evolution of secret codes and the role of cryptography in securing information. The historical review of substitution ciphers, one of the foundational concepts in cryptography, offers insights into how encryption and decryption techniques have developed over time.

6. Tools and Languages

Tools :

- Visual Studios
- Notepad++

Languages :

- Html
- CSS
- Script

7. Process

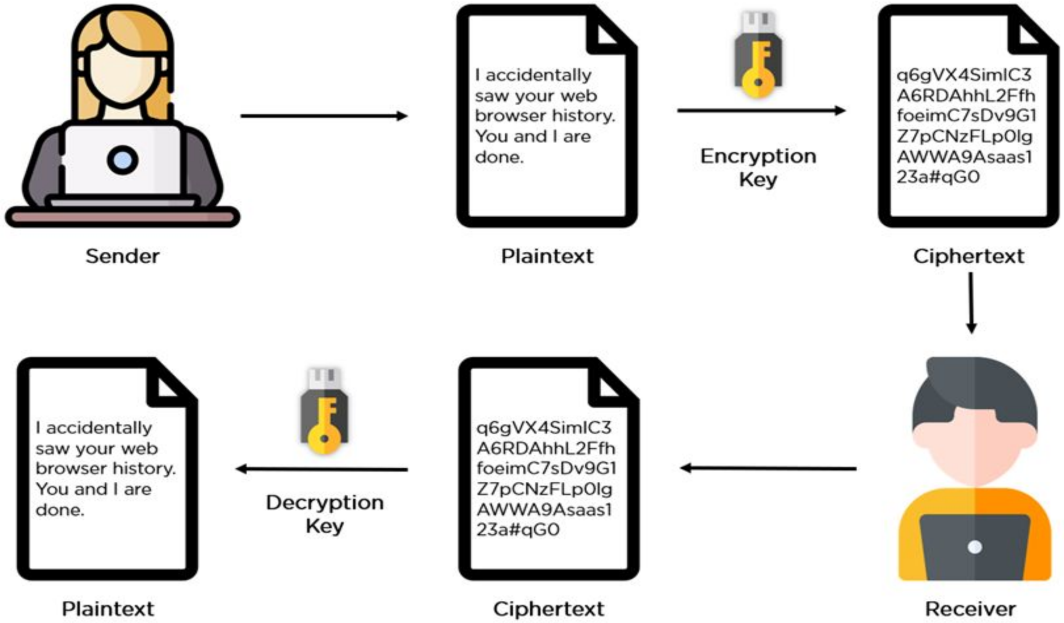
Encryption:

- Prepare the Plaintext that we’ve to convert into Ciphertext.
- Choose a Key.
- Encrypt the given text.
- We’ll get the Ciphertext.

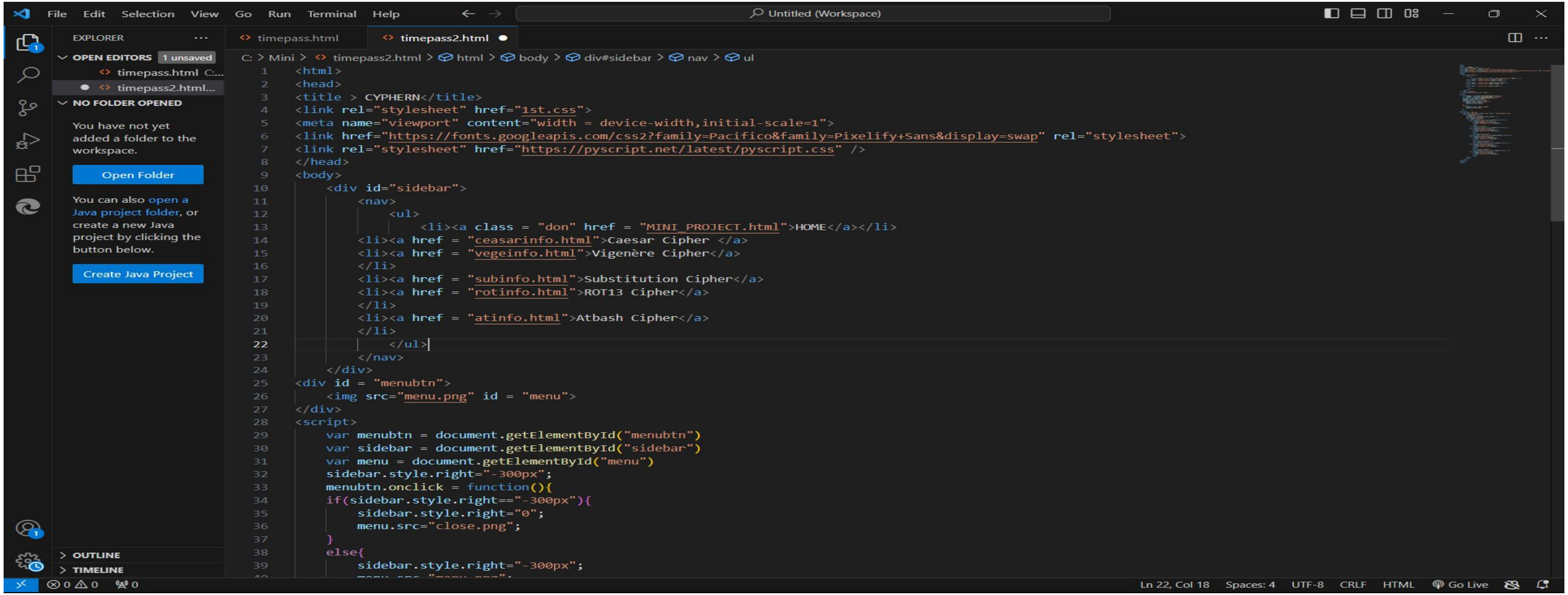
Decryption:

- Prepare the Ciphertext to convert it into Plaintext.
- Choose the same Key.
- Decrypt the Text.
- We’ll Get the original Plaintext.

8.Architecture


Sender
I accidentally saw your web browser history. You and I are done.
Plaintext
Encryption Key
q6gVX4SimIC3 A6RDAhhL2Ffh foeimC7sDv9G1 Z7pCNzFLp0lg AWWA9Asaas1 23a#qG0
Ciphertext
Receiver
q6gVX4SimIC3 A6RDAhhL2Ffh foeimC7sDv9G1 Z7pCNzFLp0lg AWWA9Asaas1 23a#qG0
Ciphertext
Decryption Key
I accidentally saw your web browser history. You and I are done.
Plaintext

9. Implementation

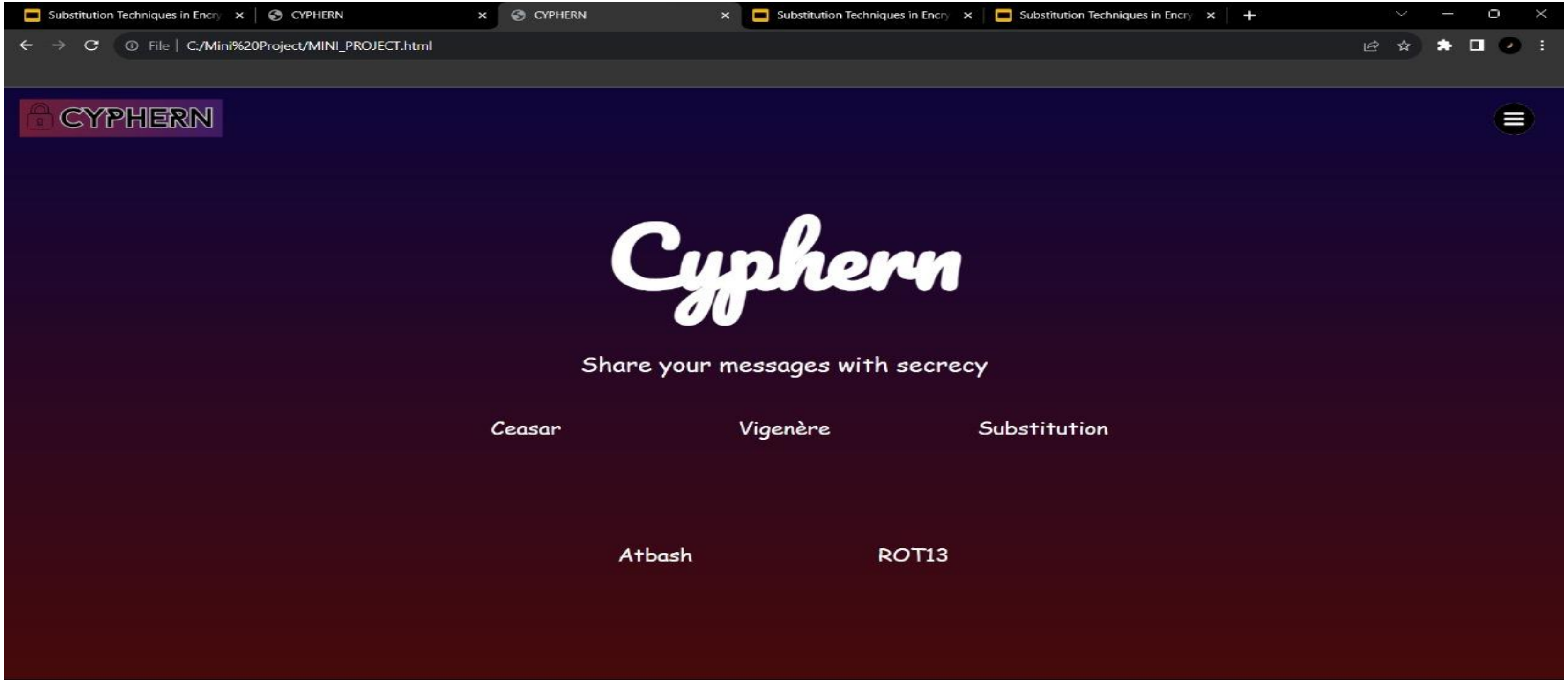


You have not yet added a folder to the workspace.

You can also open a Java project folder, or create a new Java project by clicking the button below.

```html
<html>
<head>
<title > CYPHERN</title>
<link rel="stylesheet" href="1st.css">
<meta name="viewport" content="width = device-width,initial-scale=1">
<link href="https://fonts.googleapis.com/css2?family=Pacifico&family=Pixelify+Sans&display=swap" rel="stylesheet">
<link rel="stylesheet" href="https://pyscript.net/latest/pyscript.css" />
</head>
<body>
    <div id="sidebar">
        <nav>
            <ul>
                <li><a class = "don" href = "MINI_PROJECT.html">HOME</a></li>
        <li><a href = "ceasarinfo.html">Caesar Cipher </a>
        <li><a href = "vegeinfo.html">Vigenère Cipher</a>
        </li>
        <li><a href = "subinfo.html">Substitution Cipher</a>
        <li><a href = "rotinfo.html">ROT13 Cipher</a>
        </li>
        <li><a href = "atinfo.html">Atbash Cipher</a>
        </li>
            </ul>
        </nav>
    </div>
<div id = "menubtn">
    <img src="menu.png" id = "menu">
</div>
<script>
    var menubtn = document.getElementById("menubtn")
    var sidebar = document.getElementById("sidebar")
    var menu = document.getElementById("menu")
    sidebar.style.right="-300px";
    menubtn.onclick = function(){
    if(sidebar.style.right=="-300px"){
        sidebar.style.right="0";
        menu.src="close.png";
    }
    else{
        sidebar.style.right="-300px";
```

10. Interface



Substitution Techniques in Encry
CYPHERN
CYPHERN
Substitution Techniques in Encry
Substitution Techniques in Encry
File | C:/Mini%20Project/MINI_PROJECT.html
CYPHERN
Cyphern
Share your messages with secrecy
Ceasar
Vigenère
Substitution
Atbash
ROT13

11. Results

Educational Resources:

If your project is educational in nature, the main result may be the creation of valuable educational resources.

Research Findings:

Your project may result in research findings and conclusions about the various substitution techniques.

User Documentation:

If you've developed software, user documentation explaining how to use the software and understand the principles of substitution ciphers will be a vital result.

12. List of Publications

- Google Scholar
- IEEE Xplore
- ACM Digital Library
- ScienceDirect
- JSTOR
- SpringerLink
- ResearchGate

13. Conclusion and Future Work

Conclusion:

Substitution techniques in encryption and decryption involve replacing characters in a message to protect information. They are basic, historically significant, and useful for simple security but not suitable for highly sensitive data. Modern cryptography relies on more advanced methods for robust security.

Future Work:

- ɪmprove substitution algorithms.
- Explore machine learning applications.
- Publish Website
- Premium membership

References

- Cryptography: Theory and Practice by Douglas R. Stinson (2006)
- Cryptography and Network Security: Principles and Practice by William Stallings (2011)
- Substitution Techniques: Basics and Advances by Santanu Kumar Das, Bijoy Krishna Roy, and Palash Dutta (2017)
- Substitution Techniques for Data Protection: A Comprehensive Survey by Abhilasha Maurya and Dr. Rajesh Kumar Singh (2019)
- Substitution Technique in Cryptography by International Journal of Advanced Research in Computer Science and Engineering (IJARCSE) (2018)

Thank You