King Abdulaziz University
Faculty of Computing & Information
TechnologyComputer Science Department

CPCS 425: Information Security

Project: Cipher Application

Saturday 18th of Novembre 2023

Prepared for:

Dr. Reemah Alhebshi

Student	ID	Section
Reem Alqarni	2005297	GAR

Table Of Content

1. Introduction

Encryption is a fundamental concept in the field of computer security and information protection. It involves the transformation of data into a format that is unintelligible and scrambled, known as ciphertext, using an algorithm and a key. The purpose of encryption is to ensure the confidentiality and integrity of sensitive information, making it unreadable to unauthorized individuals.

The process of encryption involves converting plaintext, which is the original readable data, into ciphertext using an encryption algorithm and a secret encryption key. The encryption algorithm performs a series of mathematical operations on the plaintext, scrambling it according to the specific encryption scheme. The encryption key, which is a unique parameter, determines the transformation applied by the algorithm and is required to decrypt the ciphertext back into its original form. By encrypting data, even if it is intercepted or accessed by unauthorized parties, it remains unreadable and meaningless without the corresponding decryption key. Encryption provides a secure method of protecting sensitive information during storage, transmission, or communication, guarding against unauthorized access, data breaches, and other security risks. Encryption finds wide application in various domains, including secure communication over networks, protecting personal and financial data in online transactions, securing files and documents, and safeguarding sensitive information in government, military, and corporate environments. Different encryption algorithms and protocols exist, each with its own strengths and weaknesses, and the choice of algorithm depends on factors such as security requirements, performance, and compatibility.

It is important to note that encryption does not guarantee absolute security, as vulnerabilities can be discovered or keys can be compromised. However, encryption plays a crucial role in maintaining the confidentiality and integrity of sensitive data, forming a critical component of modern security practices.

2. Difference between encryption and decryption

Encryption and decryption are two complementary processes used to secure and retrieve sensitive information. Let's explore each process in more detail.

2.1 Encryption

Encryption is the process of transforming plaintext (readable data) into ciphertext (scrambled data) using an encryption algorithm and a secret encryption key. The encryption algorithm performs a series of mathematical operations on the plaintext, making it incomprehensible to unauthorized individuals. The encryption key is a unique parameter that determines the transformation applied by the algorithm.

The goals of encryption are to ensure confidentiality and data integrity. By encrypting data, even if it is intercepted or accessed without authorization, it remains unreadable and meaningless. Encryption protects sensitive information during storage, transmission, or communication, guarding against unauthorized access and data breaches.

2.2 Decryption

Decryption is the reverse process of encryption. It involves converting ciphertext back into plaintext using a decryption algorithm and the corresponding decryption key. The decryption algorithm applies the reverse operations of the encryption algorithm, effectively reversing the transformation and restoring the original plaintext.

Decryption is performed by authorized individuals who possess the correct decryption key. With the key, they can convert the ciphertext back into its original readable form, allowing access to the protected information.

Together, encryption and decryption form a cryptographic system that enables secure communication, data protection, and information security. These processes are utilized in various domains, including secure messaging, online transactions, file storage, virtual private networks (VPNs), and more.

It is essential to use strong encryption algorithms and protect the secrecy of encryption keys to maintain the security of encrypted data. Additionally, encryption protocols and best practices are continuously evolving to address new threats and vulnerabilities.

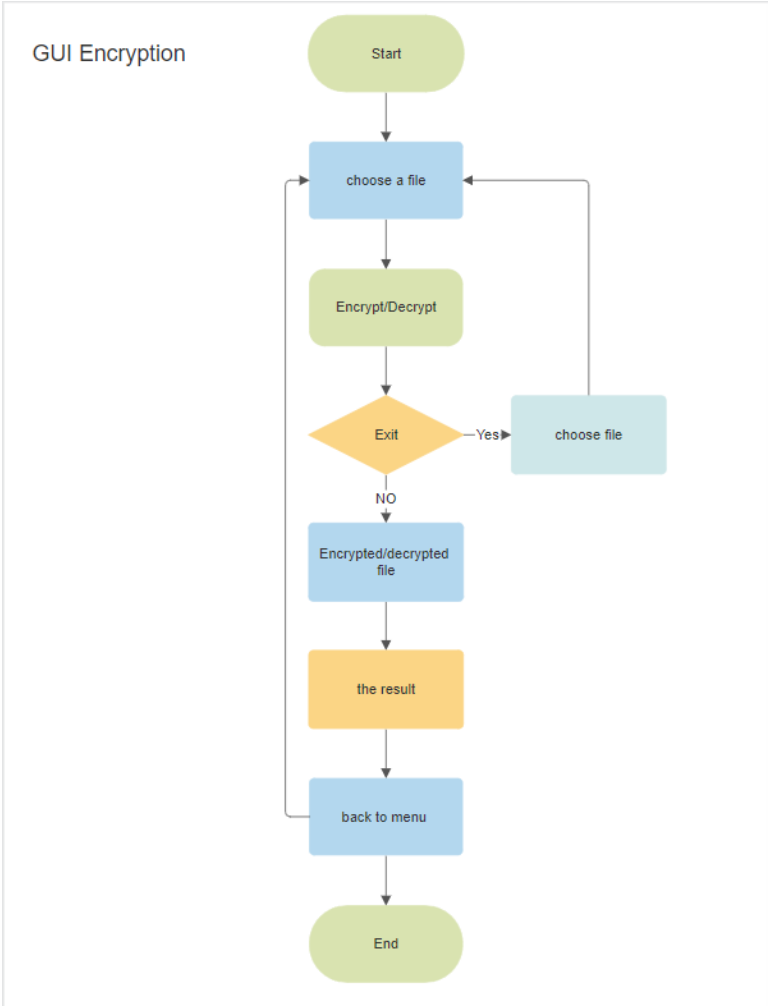
By employing encryption and decryption techniques effectively, organizations and individuals can safeguard their sensitive information, maintain privacy, and mitigate the risks associated with unauthorized access. In this project we will illustrate the technique that we used for this project and hoe encrypt and decrypt the code.

3. The pseudocode of encryption and decryption

```
// Pseudocode for Encryption Method
function encrypt(inputFile, outputFile):
    try:
        open inputFile for reading
        open outputFile for writing
        for each line in inputFile:
            trim the line and convert to uppercase
            perform swapping based on length
            perform additional swapping if length is greater than or equal to 4
            replace specific characters with corresponding symbols
            write the result to outputFile
        close inputFile and outputFile
    catch FileNotFoundException:
        print error message
--------------------------------------------------------------------------------
// Pseudocode for Decryption Method
function decrypt(inputFile, outputFile):
    try:
        open inputFile for reading
        open outputFile for writing
        for each line in inputFile:
            replace symbols with corresponding characters
            trim the line
            perform swapping based on length
            perform additional swapping if length is greater than or
equal to 4
            convert the result to lowercase
            write the result to outputFile
        close inputFile and outputFile
    catch FileNotFoundException:
        print error message
```

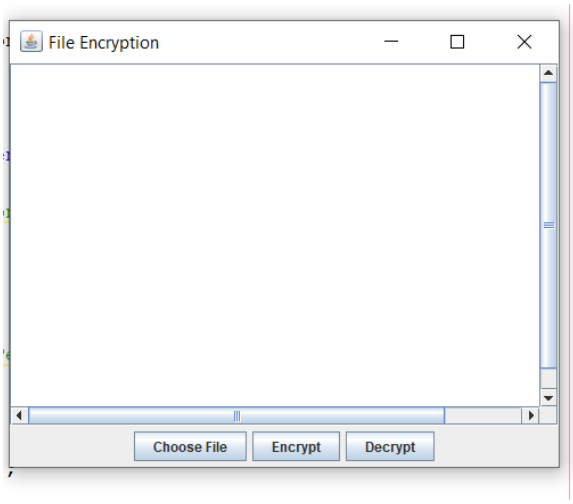
```
-------------------------------------------------------------------------
// Pseudocode for Main calling
call encrypt method with inputFile and outputFile as parameters
call decrypt method with inputFile2 and outputFile2 as parameters
```

4. Flowchart

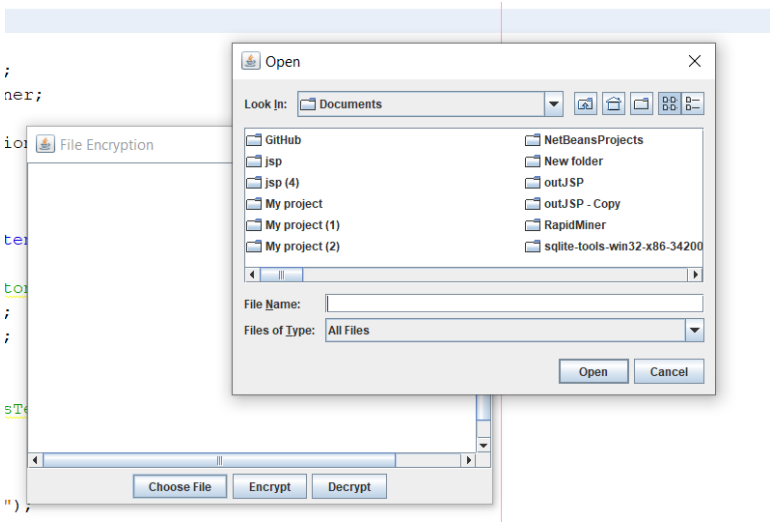


5. Output

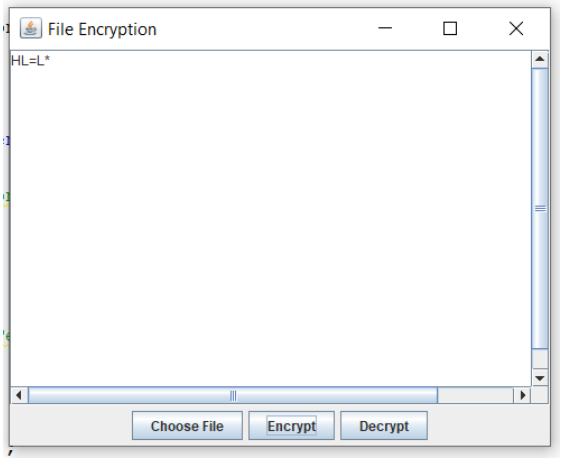
1- The interface



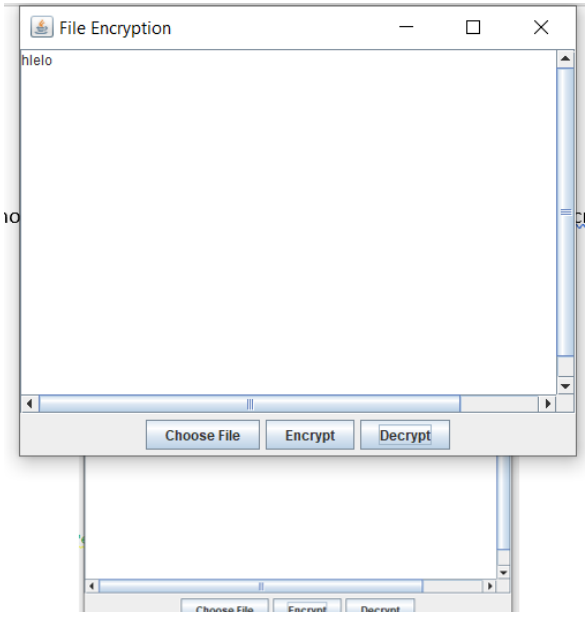
2- choose file from the device I choose plain.txt file that has the word (Hello).



3- After choosing the file press whatever you want here I went for “ Encrypt” .



4- Here after the encryption I choose “ Decrypt” .



6. Conclusion

In conclusion, encryption and decryption are critical components of modern information security systems. They enable secure communication, protect sensitive data, and ensure the confidentiality, integrity, and authenticity of information. However, it is essential to stay vigilant, keep up with advancements in encryption technologies, and follow best practices to mitigate potential vulnerabilities and adapt to evolving threats. In this project we learned how to do a small application of encryption and decryption. And that was so useful.