

[This Photo](https://jpralves.net/post/2019/03/14/breakthrough-research-using-quantum-cryptography-addresses-security-in-5g-networks.html) by Unknown Author is licensed under [CC BY-NC-ND](https://creativecommons.org/licenses/by-nc-nd/3.0/)

Cryptography Application

First C++ Projects

**S.L.S Machipi 50713965 | CMPG 121 | 6 October 2024**

Contents

[Program Scope 2](#_Toc179036999)

[Cryptography Application 2](#_Toc179037000)

[Functionality 2](#_Toc179037001)

[Technical Requirements 3](#_Toc179037002)

[Advanced Requirements: 3](#_Toc179037003)

[Pseudocode 4](#_Toc179037004)

[Flowcharts 6](#_Toc179037005)

[Research on Advanced requirements 7](#_Toc179037006)

[References 8](#_Toc179037007)

# Program Scope

## Cryptography Application

Cryptography is a method of protecting information and communications using codes, so that only those for whom the information is intended can read and process it.

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

The program I will develop is a Cryptography Application that allows users to encrypt and decrypt messages using simple algorithms. The intended users are individuals interested in learning about basic cryptographic techniques and securing their messages.

### Functionality

* Users can input a message to be encrypted or decrypted.
* The application will use a struct to define a Message that contains the original text, encrypted text, and a key.
* Users can choose between different encryption methods (e.g., Caesar cipher, substitution cipher).
* The program will provide options to save encrypted messages to a file and load them back for decryption.
* The application will manage errors gracefully, ensuring valid inputs and providing feedback to the user.

### Technical Requirements

* Implementing an array to store the alphabet.
* Using structs to define a Cipher structure that holds the original and encrypted characters.
* Defining at least three functions: one for encryption, one for decryption, and one for user interaction.
* Utilizing conditional statements to manage user choices.
* Implementing loops for processing input and output.
* Incorporating file handling to save and load messages.
* Handling errors through input validation.

### Advanced Requirements:

* Use a class Cipher Tool to encapsulate the encryption and decryption logic.
* Implement smart pointers to manage memory for dynamically allocated objects.
* Utilize generic templates for handling several types of data in the program.

# Pseudocode

START

DEFINE struct Cipher.

char original

char encrypted

DEFINE class CipherTool

PRIVATE

array<Cipher> cipherArray

PUBLIC

FUNCTION encrypt(message)

FUNCTION decrypt(message)

FUNCTION loadCipherFromFile(filename)

FUNCTION saveCipherToFile(filename)

FUNCTION main()

DISPLAY "Welcome to the Cryptography Tool"

WHILE true

DISPLAY "1. Encrypt a message"

DISPLAY "2. Decrypt a message"

DISPLAY "3. Exit"

GET userChoice

IF userChoice == 1 THEN

GET message

encryptedMessage = CipherTool.encrypt(message)

DISPLAY encryptedMessage

ELSE IF userChoice == 2 THEN

GET message

decryptedMessage = CipherTool.decrypt(message)

DISPLAY decryptedMessage

ELSE IF userChoice == 3 THEN

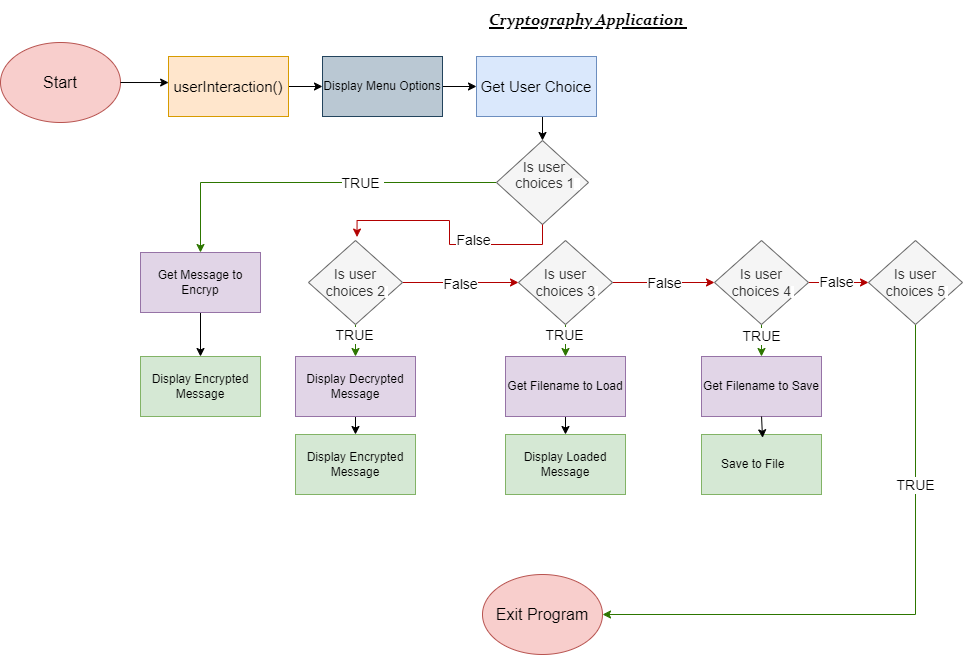
BREAK

ELSE

DISPLAY "Invalid choice, please try again"

END

# Flowcharts



# Research on Advanced requirements

* **Classes and Objects:** Classes in C++ allow for encapsulation of data and functions. The Cipher Tool class will encapsulate all functionalities related to encryption and decryption, making the code modular and easier to maintain.
* **Smart Pointers:** Smart pointers, such as “***unique\_ptr,”*** manage memory automatically, preventing memory leaks. They will be used in the Cipher Tool class to manage dynamically allocated arrays for the cipher.
* **Generic Templates:** Templates allow functions and classes to operate with any data type. This will be useful for creating a flexible Cipher Tool that can manage several types of messages (e.g., strings, character arrays).

# References

1. Kjell, B. (2024). Functions. [online] Ccsu.edu. Available at: https://chortle.ccsu.edu/StructuredC/Chap03/struct03\_16.html#:~:text=In%20flowcharts%2C%20a%20function%20call [Accessed 30 Sep. 2024].
2. GeeksforGeeks. (2020). Class Diagram for Library Management System. [online] Available at: <https://www.geeksforgeeks.org/class-diagram-for-library-management-system/>.
3. www.programiz.com. (n.d.). C++ Pointers. [online] Available at: <https://www.programiz.com/cpp-programming/pointers>.
4. Apperson, L. (2024). Advanced Topics in C++ - Lem Apperson - Medium. [online] Medium. Available at: https://medium.com/@lemapp09/advanced-topics-in-c-57d759a1c085 [Accessed 30 Sep. 2024].