Математические основы защиты информации и информационной безопасности.

Лабораторная работа №1.

Подмогильный Иван Александрович.

Содержание

List of Figures

List of Tables

1 Цель работы

Освоить на практике шифрование шифров Цезаря и Атбаша.

2 Задание

1. Реализовать шифр Цезаря
2. Реализовать шифр Атбаш

3 Выполнение лабораторной работы

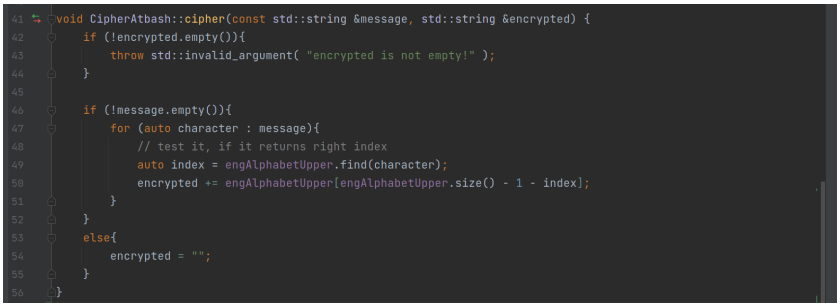
Написал код для зашивровки кодов шифром Цезаря

Figure 3.1: Caesar cipher

Написал код для дешивровки кодов шифром Цезаря

Figure 3.2: Caesar decipher

Написал код для зашивровки кодов шифром Атбаша



```cpp
void CipherAtbash::cipher(const std::string &message, std::string &encrypted) {
    if (!encrypted.empty()){
        throw std::invalid_argument( "encrypted is not empty!" );
    }

    if (!message.empty()){
        for (auto character : message){
            // test it, if it returns right index
            auto index = engAlphabetUpper.find(character);
            encrypted += engAlphabetUpper[engAlphabetUpper.size() - 1 - index];
        }
    }
    else{
        encrypted = "";
    }
}
```

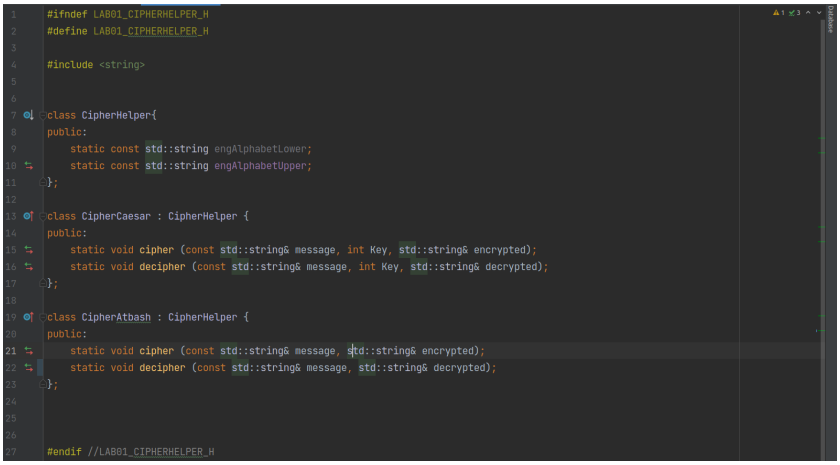
Figure 3.3: Atbash cipher

Написал код для дешивровки кодов шифром Атбаша

```cpp
void CipherAtbash::decipher(const std::string &message, std::string &decrypted) {
    cipher(message, &decrypted);
}
```

Figure 3.4: Atbash decipher

Написал заголовочный файл для класса реализации CipherHelper



```cpp
#ifndef LAB01_CIPHERHELPER_H
#define LAB01_CIPHERHELPER_H

#include <string>


class CipherHelper{
public:
    static const std::string engAlphabetLower;
    static const std::string engAlphabetUpper;
};

class CipherCaesar : CipherHelper {
public:
    static void cipher (const std::string& message, int Key, std::string& encrypted);
    static void decipher (const std::string& message, int Key, std::string& decrypted);
};

class CipherAtbash : CipherHelper {
public:
    static void cipher (const std::string& message, std::string& encrypted);
    static void decipher (const std::string& message, std::string& decrypted);
};



#endif //LAB01_CIPHERHELPER_H
```

Figure 3.5: Header file

Написал CMakeLists.txt файл, который создаёт библиотеку из класса CipherHelper и бинарник main

```
cmake_minimum_required(VERSION 3.20)
project(lab01)

set(CMAKE_CXX_STANDARD 14)

add_library(lab01 src/CipherHelper.cpp)

add_executable(main src/main.cpp)
target_link_libraries(main lab01)
```

Figure 3.6: CmakeLists.txt file

Написал main.cpp файл, в котором есть тесты реализованных функций. Часть шифра Цезаря:

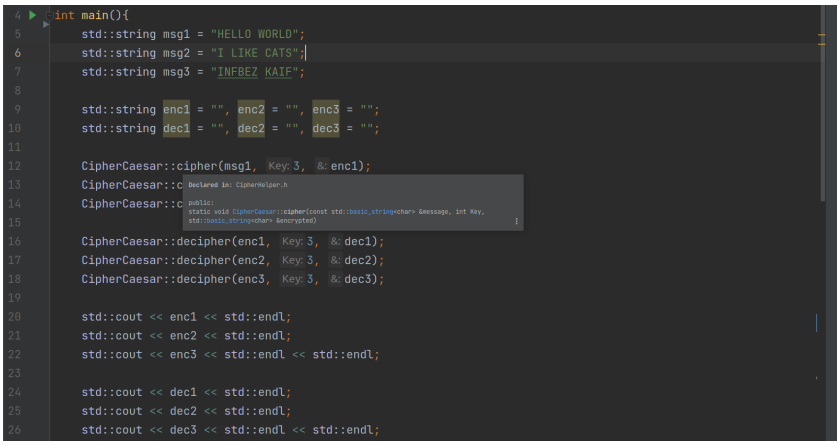


Figure 3.7: main.cpp

Часть шифра Атбаша:

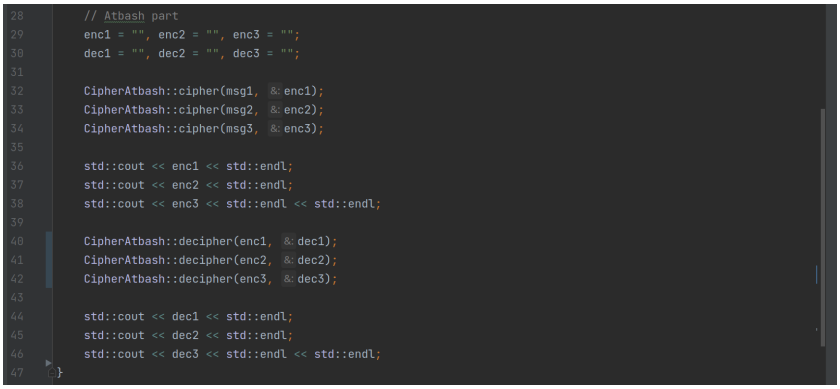


Figure 3.8: main.cpp

Результаты тестов. Первые три строчки это зашифрованные сообщения шифром Цезаря. Следующие три строчки, это расшифрованные сообщения. Следующие три строчки, это те же сообщения, но зашифрованные шифром Атбаш. И последние три строчки - расшифрованные сообщения.

Figure 3.9: tests

4 Выводы

Освоил на практике применение методов шифрования Цезаря и Атбаша.