Математические основы защиты информации и информационной безопасности.

Лабораторная работа №1.

Селезнев Василий 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

```cpp
#include "../include/CipherHelper.h"

#include <iostream>

//const std::string CipherHelper::engAlphabetLower = "abcdefghijklmnopqrstuvwxyz";
const std::string CipherHelper::engAlphabetUpper = "ABCDEFGHIJKLMNOPQRSTUVWXYZ ";

void CipherCaesar::cipher(const std::string& message, int Key, std::string& encrypted){
    // char with index j => char with index (j + k) / mod 26
    if (!encrypted.empty()){
        throw std::invalid_argument( s: "encrypted is not empty!" );
    }

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

Figure 3.1: Caesar cipher

Написал код для дешивровки кодов шифром Цезаря

```cpp
void CipherCaesar::decipher(const std::string &message, int Key, std::string &decrypted) {
    if (!decrypted.empty()){
        throw std::invalid_argument( s: "decrypted is not empty!" );
    }

    if (!message.empty()){
        for (auto character :char : message){
            auto index :  = engAlphabetUpper.find( c: character);
            decrypted += engAlphabetUpper[ (engAlphabetUpper.size() +  (index - Key)) % engAlphabetUpper.size() ];
        }
    }
    else{
        decrypted = "";
    }
}
```

Figure 3.2: Caesar decipher

Написал код для зашивровки кодов шифром Атбаша

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

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

Figure 3.3: Atbash cipher

Написал код для дешивровки кодов шифром Атбаша

```
void CipherAtbash::decipher(const std::string &message, int Key, std::string &decrypted) {
    if (!decrypted.empty()){
        throw std::invalid_argument( s: "decrypted is not empty!" );
    }
```

Figure 3.4: Atbash decipher

Написал заголовочный файл для класса реализации CipherHelper

```
#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, int Key, 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:

```cpp
int main(){

    // Caesar part

    std::string msg1 = "MY NAME IS VASYA";
    std::string msg2 = "I LOVE STUDY";
    std::string msg3 = "RUDN IS THE BEST UNIVERSITY";

    std::string enc1 = "", enc2 = "", enc3 = "";
    std::string dec1 = "", dec2 = "", dec3 = "";

    CipherCaesar::cipher( message: msg1,  Key: 3,  &: enc1);
    CipherCaesar::cipher( message: msg2,  Key: 3,  &: enc2);
    CipherCaesar::cipher( message: msg3,  Key: 3,  &: enc3);

    CipherCaesar::decipher( message: enc1,  Key: 3,  &: dec1);
    CipherCaesar::decipher( message: enc2,  Key: 3,  &: dec2);
    CipherCaesar::decipher( message: enc3,  Key: 3,  &: dec3);

    std::cout << enc1 << std::endl;
    std::cout << enc2 << std::endl;
    std::cout << enc3 << std::endl << std::endl;

    std::cout << dec1 << std::endl;
    std::cout << dec2 << std::endl;
    std::cout << dec3 << std::endl << std::endl;
```

Figure 3.7: main.cpp

Часть шифра Атбаша:

```
    enc1 = "", enc2 = "", enc3 = "";
    dec1 = "", dec2 = "", dec3 = "";

    CipherAtbash::cipher( message: msg1,  &: enc1);
    CipherAtbash::cipher( message: msg2,  &: enc2);
    CipherAtbash::cipher( message: msg3,  &: enc3);

    std::cout << enc1 << std::endl;
    std::cout << enc2 << std::endl;
    std::cout << enc3 << std::endl << std::endl;

    CipherAtbash::cipher( message: enc1,  &: dec1);
    CipherAtbash::cipher( message: enc2,  &: dec2);
    CipherAtbash::cipher( message: enc3,  &: dec3);

    std::cout << dec1 << std::endl;
    std::cout << dec2 << std::endl;
    std::cout << dec3 << std::endl << std::endl;




}
```

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.

```
/Users/vasyaseleznev/infbez/lab01/cmake-build-debug/main
PACQDPHCLVCYDVAD
LCORYHCVWXGA
UXGQCLVCWKHCEHVWCXQLYHUVLWA

MY NAME IS VASYA
I LOVE STUDY
RUDN IS THE BEST UNIVERSITY

OCAN OWASIAF IC
SAPMFWAIHGXC
JGXNASIAHTWAZWIHAGNSFWJISHC

MY NAME IS VASYA
I LOVE STUDY
RUDN IS THE BEST UNIVERSITY
```

Figure 3.9: tests

4 Выводы

Освоил на практике применение методов шифрования Цезаря и Атбаша.