Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н. Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н. Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

ОТЧЕТ

по лабораторной работе №1

по курсу «Защита информации»

на тему: «Шифровальная машины Энигма»

Студент ИУ7-71Б (Группа) _____ (Подпись, дата) Постнов С. А. (Фамилия И. О.)

Преподаватель _____ (Подпись, дата) Чиж И. С. (Фамилия И. О.)

2024 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Целью лабораторной работы является реализация в виде программы электронного аналога шифровальной машины «Энигма».

Для достижения поставленной цели необходимо решить следующие задачи:

1) описать принцип работы шифровальной машины;
2) спроектировать схему алгоритма работы шифровальной машины;
3) выбрать средства реализации программы;
4) разработать программу, реализующую электронный аналог шифровальной машины.

1 Аналитический раздел

1.1 Работа шифровальной машины

Шифровальная машина «Энигма» появилась в 1919 году и выглядела как портативная печатная машинка, питаемая от батареи. Оператор нажимал одну букву, и три зубчатых колеса ротора, которые менялись ежедневно, преобразовывали эту букву в другую. Далее электрические контакты создавали другие наборы перестановок, исходная буква изменялась семь раз, а потом загоралось светящееся окошко, имевшее вид буквы. Второй оператор видел эту букву, а потом передавал их группами по пять с помощью азбуки Морзе [1].

Машина включала в себя четыре отсека: три служат для роторов и один - для расположения в нем рефлектора. По своему строению ротор имел 26 сечений, по одному в соответствии каждой букве латинского алфавита; кроме этого в нем было 26 контактов, которые служат в качестве элементов соединения с другими роторами. В то время как оператор нажимает на кнопку, цепь в шифровальной машине замыкается, после чего появляется зашифрованная буква. Цепь замыкалась также при помощи рефлектора, а реализация шифровальной машины имела ряд уникальных свойств [2]:

1) зашифрованные тексты симметричны: если установить одни и те же роторы в одном и том же порядке, то повторно закодированные сообщения будут одинаковы;

2) при кодировании одинаковых и идущих друг за другом символов на выходе образуются абсолютно разные буквы;

3) предыдущее свойство обуславливало невозможность совпадения исходного и зашифрованного символов.

Вывод

В аналитическом разделе был описан принцип работы шифровальной машины «Энигма».

2 Конструкторский раздел

2.1 Схема алгоритма работы шифровальной машины

На рисунке 2.1 представлена схема алгоритма работы шифровальной машины «Энигма».

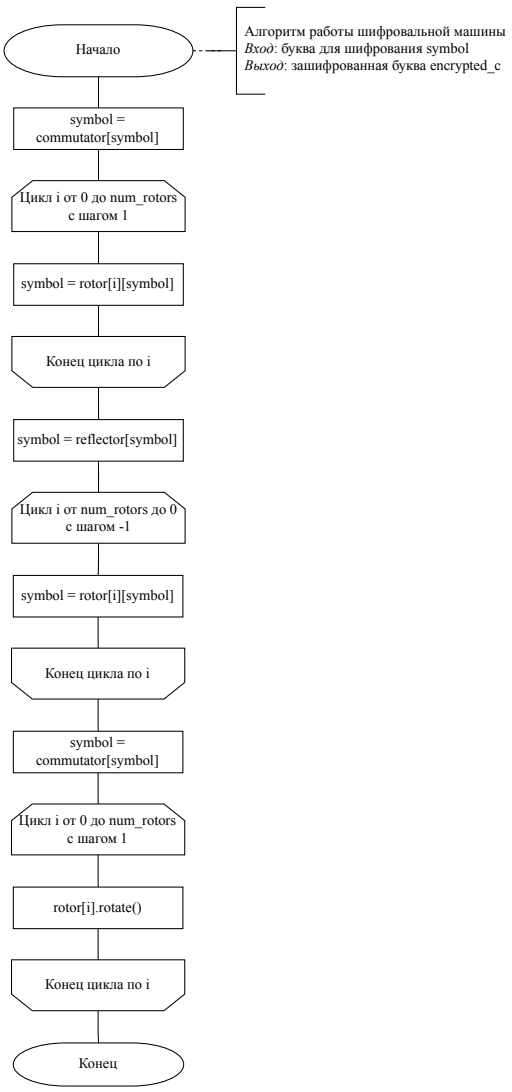

Рисунок 2.1 – Схема алгоритма работы шифровальной машины «Энигма»

Вывод

В конструкторском разделе была спроектирована схема алгоритма работы шифровальной машины «Энигма».

3 Технологический раздел

3.1 Средства реализации

Для реализации приложения был выбран язык программирования C++.

3.2 Реализация шифровальной машины «Энигма»

В листингах 3.1 – 3.4 представлен исходный код реализованной программы.

Листинг 3.1 – Исходный код класса «Энигмы»

```
#ifndef MY_ENIGMA_
#define MY_ENIGMA_

#include <string>
#include <vector>

#include "rotor.hpp"
#include "commutator.hpp"
#include "reflector.hpp"

class Enigma {
public:
    explicit Enigma(std::vector<Rotor> rotors, Reflector
       reflector, Commutator commutator, const char &min_symbol)
        : rotors(std::move(rotors)),
          commutator(std::move(commutator)),
          reflector(std::move(reflector)),
          min_symbol(min_symbol) {}

    std::string encrypt(const std::string &word) {
        std::string output;

        for (const char symbol : word) {
            // Apply the commutator
            char current_symbol = commutator.commutate(symbol -
               min_symbol) - min_symbol;

            // Forward pass through the rotors
            for (Rotor &rotor : rotors) {
                current_symbol = rotor.get_index(current_symbol
```

```
                + min_symbol);
            }

            // Apply the reflector
            current_symbol = reflector.reflect(current_symbol);

            // Reverse pass through the rotors
            for (auto it = rotors.rbegin(); it != rotors.rend();
               ++it) {
                current_symbol = it->get_symbol(current_symbol -
                   min_symbol);
            }

            // Apply the commutator again
            current_symbol = commutator.commutate(current_symbol
               - min_symbol);

            // Convert back to the character range
            output.push_back(current_symbol);

            // Rotate the rotors
            rotate_rotors();
        }

        return output;
    }

    std::string decrypt(const std::string &word) {
        reset();
        return encrypt(word);
    }

    void reset() {
        for (Rotor &rotor : rotors)
            rotor.reset();
    }
private:
    std::vector<Rotor> rotors;
    Commutator commutator;
    Reflector reflector;
```

```
    char min_symbol;

    void rotate_rotors() {
        for (auto & rotor : rotors) {
            if (rotor.rotate() != rotor.get_start()) {
                break;
            }
        }
    }
};

#endif // MY_ENIGMA_
```

Листинг 3.2 – Исходный код класса роторов «Энигмы»

```
#ifndef MY_ROTOR_
#define MY_ROTOR_

#include <vector>

class Rotor
{
public:
    explicit Rotor(const std::vector<char> &symbols, const char
       start = 0)
        : start(start), shift(start), symbols(symbols) {};

    char get_symbol(const char index) const {
        if (index >= 0 && index < symbols.size())
            return symbols[(index + shift) % symbols.size()];
        return -1;
    }

    char get_index(const char symbol) const {
        const auto it = std::find(symbols.begin(),
           symbols.end(), symbol);
        if (it != symbols.end()) {
            const char i = std::distance(symbols.begin(), it);
            return (i - shift + symbols.size()) % symbols.size();
        }
        return -1;
    }
```

```
    char get_start() const {
        return start;
    }

    char rotate()& {
        shift = (shift + 1) % symbols.size();
        return shift;
    }

    void reset() {
        shift = start;
    }
private:
    char start;
    char shift;
    std::vector<char> symbols;
};

#endif // MY_ROTOR_
```

Листинг 3.3 – Исходный код класса панели коммутации «Энигмы»

```
#ifndef MY_COMMUTATOR_
#define MY_COMMUTATOR_

#include <vector>

class Commutator
{
public:
    explicit Commutator(const std::vector<char>& symbols) :
       symbols(symbols) {};

    char commutate(const char &symbol) const {
        return symbols[symbol];
    };

private:
    std::vector<char> symbols;
};

#endif // MY_COMMUTATOR_
```

Листинг 3.4 – Исходный код класса рефлектора «Энигмы»

```
#ifndef MY_REFLECTOR_
#define MY_REFLECTOR_

#include <vector>

class Reflector
{
public:
    explicit Reflector(const std::vector<char> &s) : symbols(s)
       {};

    char reflect(const char symbol) const {
        return symbols[symbol];
    };
private:
    std::vector<char> symbols;
};

#endif // MY_REFLECTOR_
```

Вывод

В технологическом разделе были выбраны средства реализации и представлены листинги исходного кода реализованной программы.

ЗАКЛЮЧЕНИЕ

Цель работы, заключавшаяся в реализации в виде программы электронного аналога шифровальной машины «Энигма», была достигнута. Для достижения поставленной цели были решены следующие задачи:

1) описан принцип работы шифровальной машины;
2) спроектирована схема алгоритма работы шифровальной машины;
3) выбраны средства реализации программы;
4) разработана программу, реализующая электронный аналог шифровальной машины.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ОПЕРАЦИЯ БРИТАНСКОЙ РАЗВЕДКИ «ЭНИГМА». — [Электронный ресурс]. — Режим доступа: `https://www.elibrary.ru/download/elibrary_28185349_76811654.pdf` (дата обращения: 13.09.24).
2. ИССЛЕДОВАНИЕ АЛГОРИТМА РАБОТЫ ШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА». — [Электронный ресурс]. — Режим доступа: `https://human.snauka.ru/2016/06/15717` (дата обращения: 13.09.24).