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: «Электронный аналог шифровальной машины ”Энигма”»

Студент ИУ7-73Б _____ Авдейкина В. П.
(Группа) (Подпись, дата) (Фамилия И.О.)

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

2024 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Шифровальная машина «Энигма» — портативная шифровальная машина, использовавшаяся для шифрования и расшифрования секретных сообщений (семество электромеханических роторных машин, применявшихся с 1920-х годов) [1], [2].

Ротор — вращающийся диск, расположенный вдоль вала, на котором изображены символы алфавита по порядку [3]. На роторе имелись электрические контакты в количестве, равном мощности алфавита. При соприкосновении контакты соседних роторов замыкают электрическую цепь [2].

Входное колесо — колесо, соединяющее коммутационную панель или клавиатуру с роторами [2].

Рефлектор — деталь, соединяющая контакты последнего ротора попарно, коммутируя ток через роторы в обратном направлении [2]. Он обеспечивает гарантию того, что процесс расшифрования симметричен процессу шифрования, и свойство, заключающееся в том, что никакая буква не может быть зашифрована собой.

Цель данной лабораторной работы — реализация в виде программы электронного аналога шифровальной машины «Энигма».

Для достижения поставленной цели требуется решить следующие задачи:

1) описать алгоритм работы шифровальной машины «Энигма»;
2) спроектировать описанный алгоритм;
3) выбрать необходимые для разработки средства и разработать реализацию спроектированного алгоритма.

Требования к выполнению лабораторной работы:

— обеспечить шифрование и расшифровку произвольного файла, а также текстового сообщения с использованием разработанной программы;
— мощность шифруемого алфавита не должна превышать 64 символа;
— необходимо предусмотреть работу программы с пустым, однобайтовым файлом;
— должна быть возможность обработки файла архива (rar, zip или др.).

1 Аналитическая часть

Далее приведено описание работы машины «Энигма».

При каждом введении символа в машину происходят следующие действия:

1) с помощью роторов символ поочередно преобразовывается в некоторый другой символ (в прямом направлении);
2) рефлектор преобразовывает новый символ;
3) символ, полученный в результате работы рефлектора, проходит через роторы в обратном направлении;
4) итоговый символ выводится;
5) все роторы смещаются вперед на одну позицию (вращаются).

Поскольку работа машины включает в себя работу рефлектора, полученные шифрованные данные возможно синхронно расшифровать, зная настройки роторов.

2 Конструкторская часть

На рисунках 1, 2 представлены схемы алгоритмов шифрования сообщения и символа с помощью машины «Энигма» соответственно.

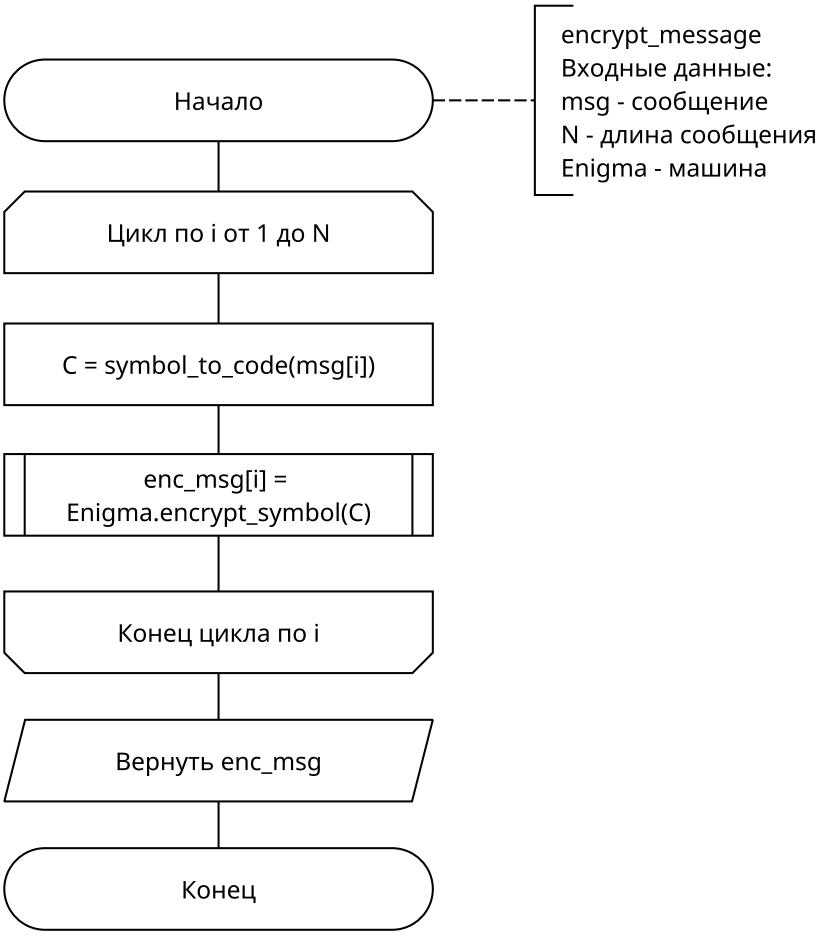

Рисунок 1 — Алгоритм шифрования сообщения

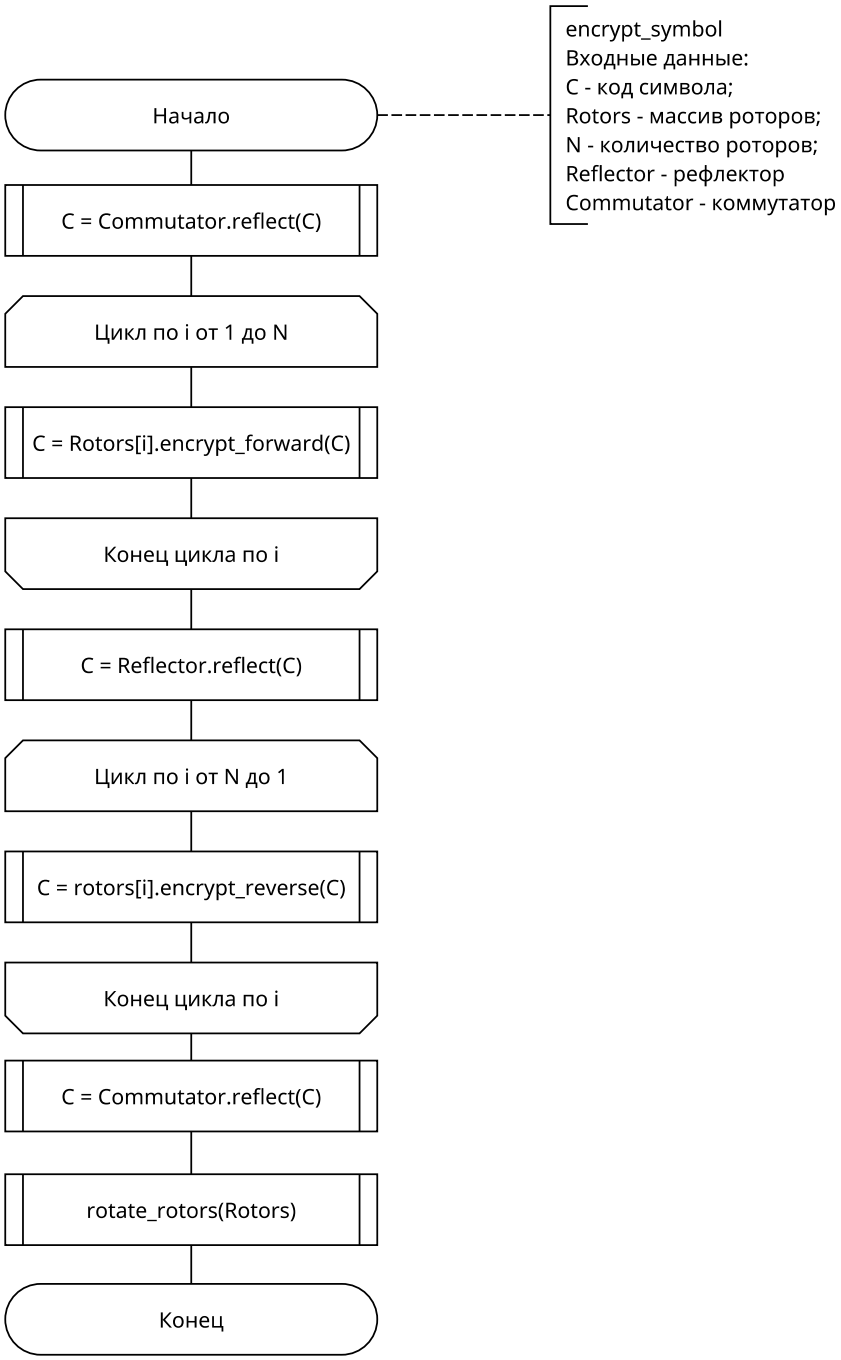

Рисунок 2 — Алгоритм шифрования символа

3 Технологическая часть

Для выполнения реализации спроектированного алгоритма был выбран язык программирования C.

На листингах 1, 2 представлены реализации алгоритмов шифрования сообщения и символа соответственно.

Листинг 1 — Алгоритм шифрования сообщения

```
std::vector<uint8_t> Enigma::encrypt(const std::string& message) {
  std::vector<uint8_t> new_message;
  for (auto &symbol: message) {
    auto new_symbol = this->encrypt(symbol);
    new_message.push_back(new_symbol);
  }
  return new_message;
}
```

Листинг 2 — Алгоритм шифрования символа

```
uint8_t Enigma::encrypt(uint8_t symbol) {
    uint64_t rotor_queue = 1;
    uint8_t new_code = this->_encoder->encode(symbol);;
    if (new_code > _size_rotor) {
        throw std::out_of_range("Code bigger than size of rotor");
    }
    new_code = _commutator[new_code];
    for (auto &rotor: _rotors) {
        new_code = rotor[new_code];
    }
    new_code = _reflector[new_code];
    for (int i = _num_rotors - 1; i >= 0; --i) {
        try {
            new_code = _find_rotor(i, new_code);
        }
        catch (const std::overflow_error& e) {
            std::cout << e.what() << std::endl;
        }
    }
    _counter++;
    for (int i = 0; i < _num_rotors; ++i) {
        if (_counter % rotor_queue == 0) {
            _rotor_shift(i);
        }
        rotor_queue *= _size_rotor;
    }
    new_code = _commutator[new_code];
    return this->_encoder->decode(new_code);
}
```

3.1 Тестирование

В таблице 1 приведены функциональные тесты (черный ящик).

Тесты пройдены успешно.

Таблица 1 — Сравнение существующих решений

Входная строка	Выходная строка
WHATISDEADMAYNEVERDIE	IVXFMCXTOHYPGYWDYFGLB
IVXFMCXTOHYPGYWDYFGLB	WHATISDEADMAYNEVERDIE
«»	«»
A	L
L	A

Так же тесты проводились на файлах, пройдены успешно.

Содержимое исходного файла: lalala

Содержимое после шифрации зашифрованного файла: lalala.

ЗАКЛЮЧЕНИЕ

Цель данной лабораторной работы — реализация в виде программы электронного аналога шифровальной машины «Энигма».

В ходе работы были выполнены следующие задачи:

1) описан алгоритм работы шифровальной машины «Энигма»;
2) спроектирован описанный алгоритм;
3) выбраны необходимые для разработки средства и разработана реализация спроектированного алгоритма.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Попов Ю. Л., Томашевский П. Р. История создания шифровальной машины «Enigma» // ББК 1 Н 34. —. — С. 1883.
2. Шолин И. М., Чубырь Н. О. АЛГОРИТМ ПЕРЕНОСНОЙ ШИФРОВАЛЬНОЙ МАШИНЫ ЭНИГМА // Форум молодых ученых. — 2018. — 10 (26). — С. 1352—1356.
3. Бабаш А. В., Баранова Е. К., Ларин Д. А. Информационная безопасность // История защиты информации в России–Москва. — 2015.