



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
(Группа)

(Подпись, дата)

Авдейкина В. П.
(Фамилия И.О.)

Преподаватель

(Подпись, дата)

Чиж И. С.
(Фамилия И.О.)

2024 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
1 Аналитическая часть	5
2 Конструкторская часть	6
3 Технологическая часть	8
ЗАКЛЮЧЕНИЕ	9
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	10

ВВЕДЕНИЕ

Шифровальная машина «Энигма» — портативная шифровальная машина, использовавшаяся для шифрования и расшифрования секретных сообщений (семейство 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.

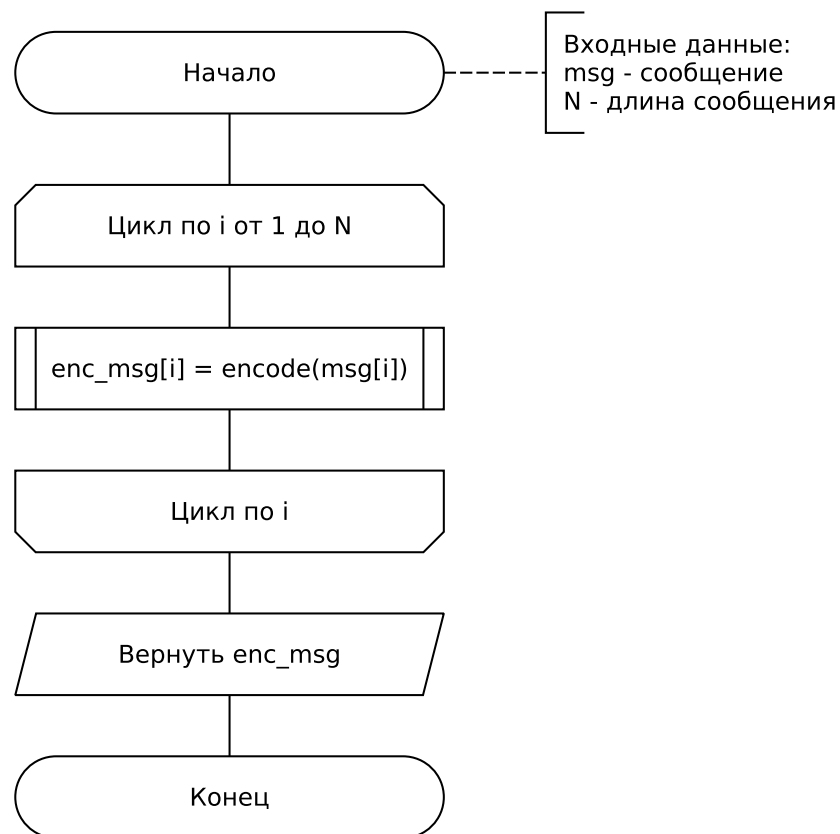


Рисунок 1 — Алгоритм шифрования сообщения

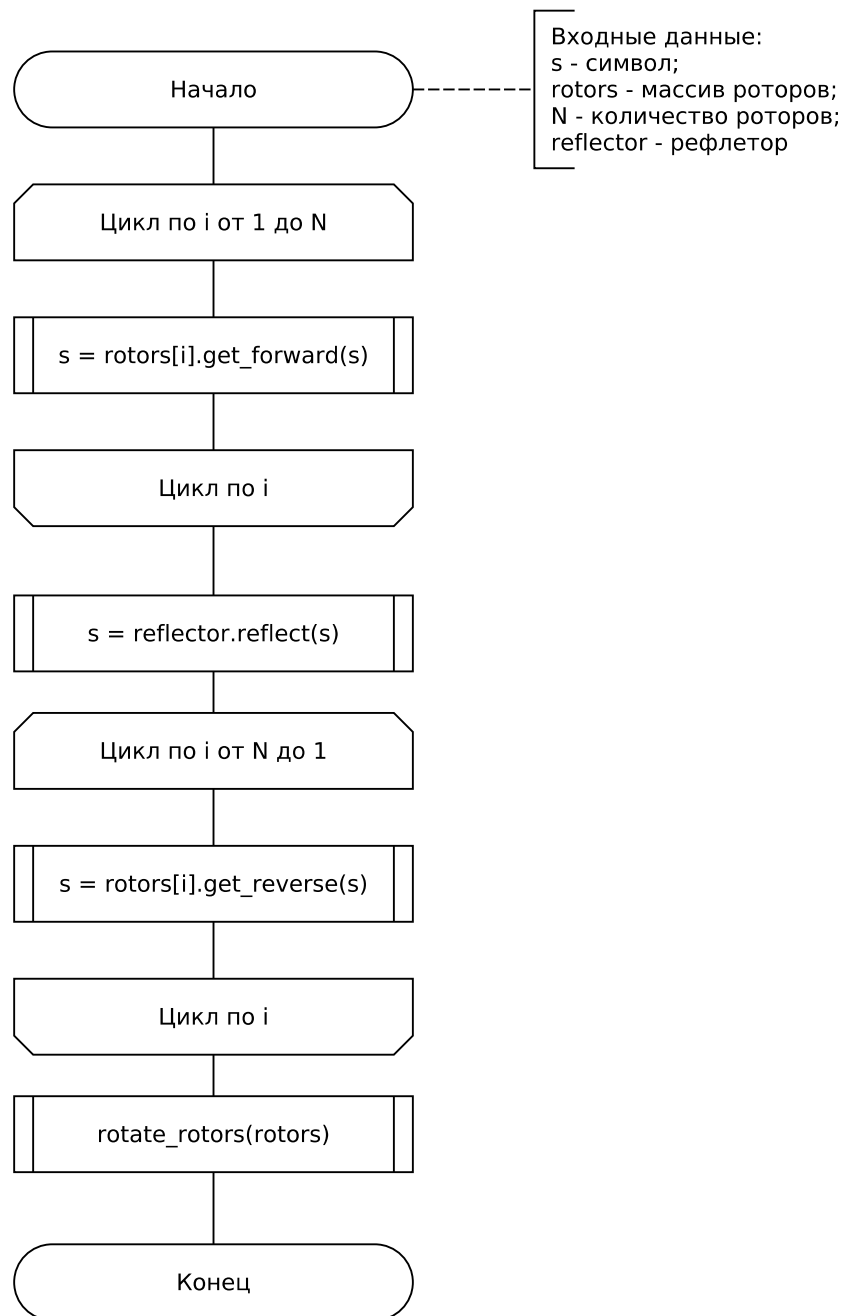


Рисунок 2 — Алгоритм шифрования символа

3 Технологическая часть

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. Бабаш А. В., Баранова Е. К., Ларин Д. А. Информационная безопасность // История защиты информации в России—Москва. — 2015.
3. Шолин И. М., Чубырь Н. О. АЛГОРИТМ ПЕРЕНОСНОЙ ШИФРОВАЛЬНОЙ МАШИНЫ ЭНИГМА // Форум молодых ученых. — 2018. — 10 (26). — С. 1352—1356.