Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

[Кафедра информационных](https://www.belstu.by/fakultety/fit/vm) систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

**Отчёт по лабораторной работе №6**

по дисциплине Информационная безопасность

Тема: Изучение устройства и функциональных особенностей шифровальной машины «Энигма»

Исполнитель:

Студент 3 курса группы 6

Руководитель:

Ассистент Нистюк О. А.

Минск, 2024

**Лабораторная работа №6**

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров.

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости перестановочных шифров.

2. Изучить структуру, принципы функционирования, реализацию процедур зашифрования сообщений в машинах семейства «Энигма».

3. Изучить и приобрести практические навыки выполнения криптопреобразований информации на платформе «Энигма», реализованной в виде симуляторов.

4. Получить практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе «Энигма».

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# Теоретические сведения

Машина «Энигма» – это электромеханическое устройство.

Как и другие роторные машины, «Энигма» состоит из комбинации механических и электрических подсистем. Механическая часть включает в себя клавиатуру, набор вращающихся дисков – роторов, которые расположены вдоль вала и прилегают к нему, и ступенчатого механизма, двигающего один или несколько роторов при каждом нажатии на клавишу. Электрическая часть, в свою очередь, состоит из электрической схемы, соединяющей между собой клавиатуру, коммутационную панель, лампочки и роторы (для соединения роторов использовались скользящие контакты).

При каждом нажатии на клавишу самый правый ротор сдвигался на одну позицию, а при определенных условиях сдвигались и другие роторы. Движение роторов приводило к различным криптографическим преобразованиям при каждом следующем нажатии на клавишу на клавиатуре, т. е. зашифрование/расшифрование сообщений основано на выполнении ряда замен (подстановок) одного символа другим.

Механические части двигались и, замыкая контакты, образовывали меняющийся электрический контур. При нажатии на клавишу клавиатуры контур замыкается, ток проходит через созданную (для зашифрования/расшифрования одного конкретного символа сообщения) цепь и в результате включает одну из набора лампочек, отображающую искомую букву шифртекста (или расшифрованного сообщения).

# Ход работы

Целью работы была разработка приложения-симулятора шифровальной машины «Энигма», состоящей из клавиатуры, трех роторов и отражателя. Для этого был разработан класс Enigma.

Метод rotorEncrypt принимает на вход шифруемый символ алфавита, алфавит из которого будет осуществляться преобразования, алфавит в который будет осуществляться преобразование (алфавит ротора) и текущее смещение ротора. Код метода представлен на рисунке 2.1.

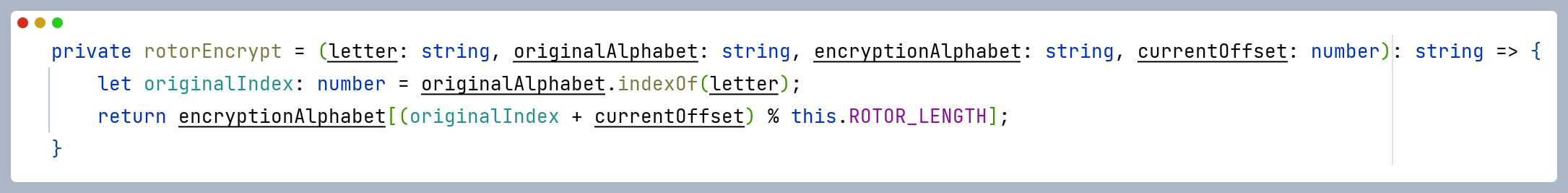


Рисунок 2.1 – Код метода шифрования символа с помощью ротора

Далее были разработаны методы directPath и reversePath, которые представляют собой прямой и обратный пути преобразования соответственно. Код методов представлен на рисунке 2.2.



Рисунок 2.2 – Код методов прямого и обратного пути зашифрования/расшифрования

Метод passThroughReflector принимает текущий символ и осуществляет подстановку на основе B Dunn рефлектора. Код метода представлен на рисунке 2.3.

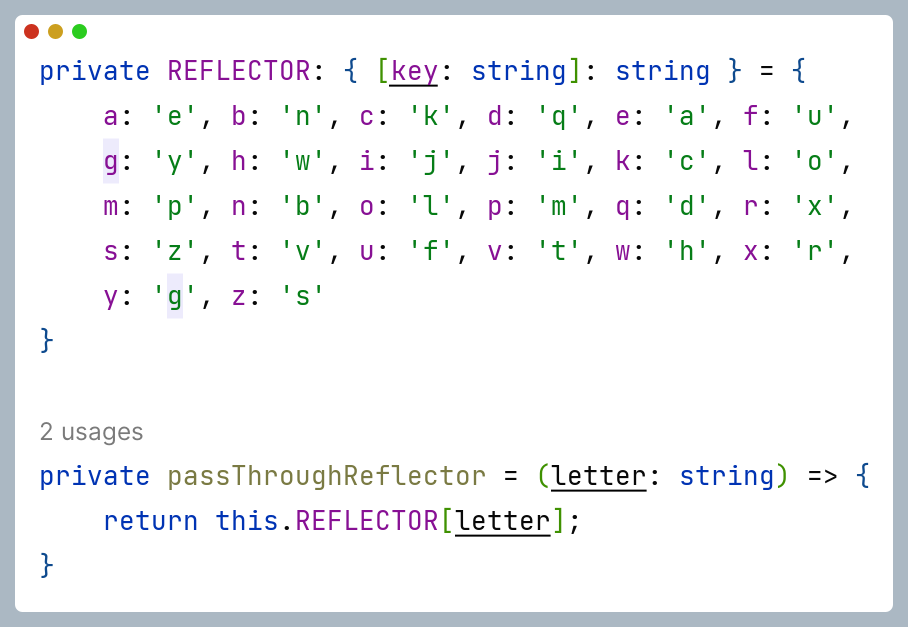


Рисунок 2.3 – Код метода рефлектора

Метод shiftRotors выполняется после зашифрования/расшифрования одного символа и меняет положения каждого из роторов. Код метода представлен на рисунке 2.4.

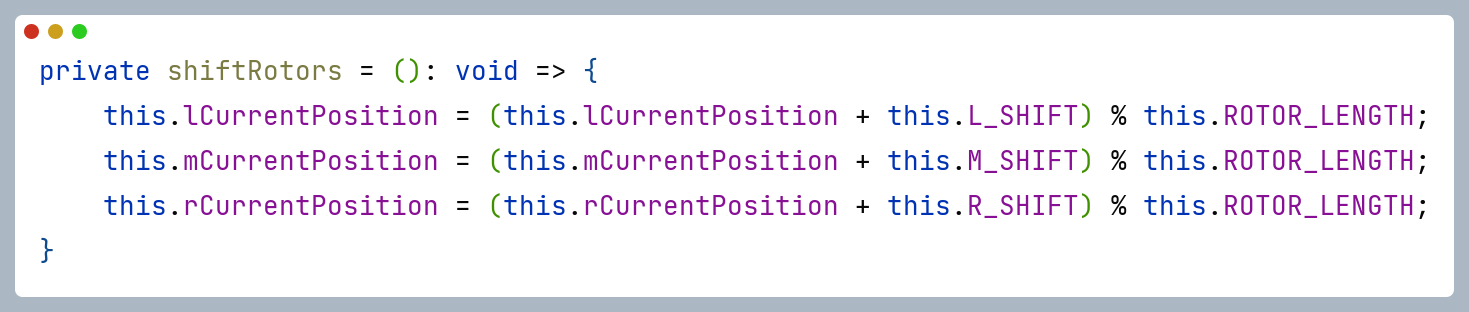


Рисунок 2.3 – Код метода, смещающего роторы

Итоговый метод шифрования encrypt принимает на вход оригинальный текст и выполняет шифрование с помощью метода прямого пути, метода рефлектора и метода обратного пути. После каждой итерации осуществляется смещение роторов. Код метода представлен на рисунке 2.4.

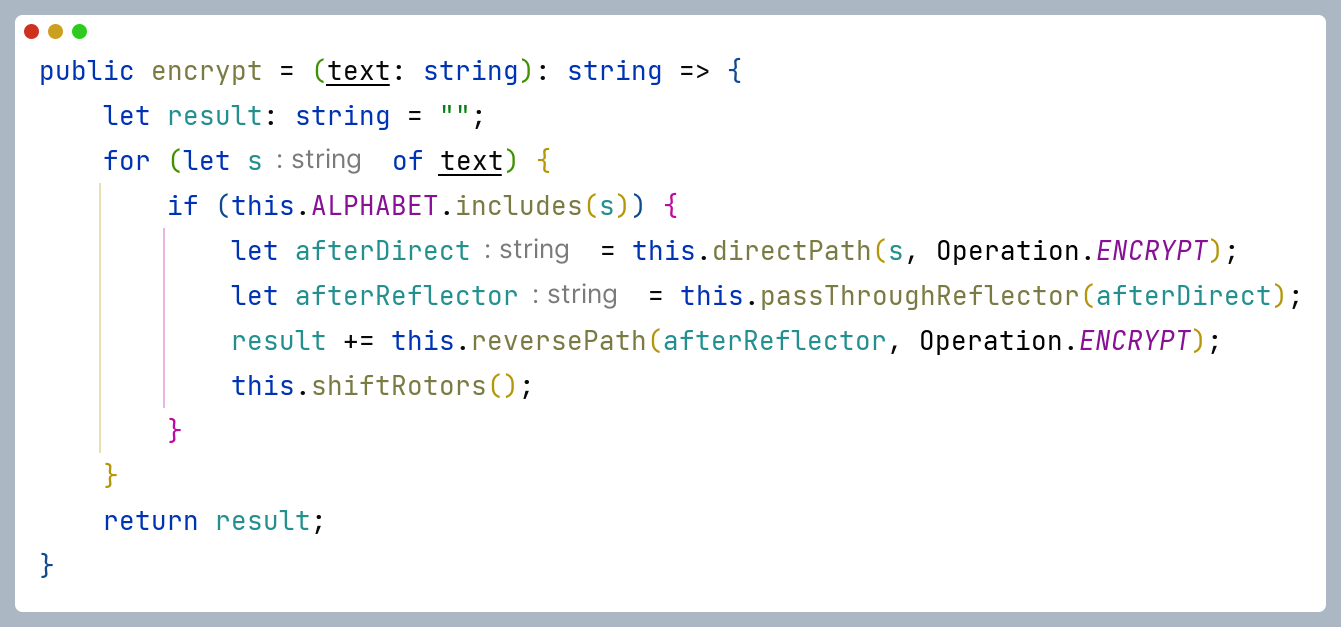


Рисунок 2.4 – Код метода шифрования

Метод расшифрования decrypt принимает на вход зашифрованный текст. Он выполняет аналогичные методу encrypt операции, только на прямом и обратном пути осуществляет расшифрование. Код метода представлен на рисунке 2.5.

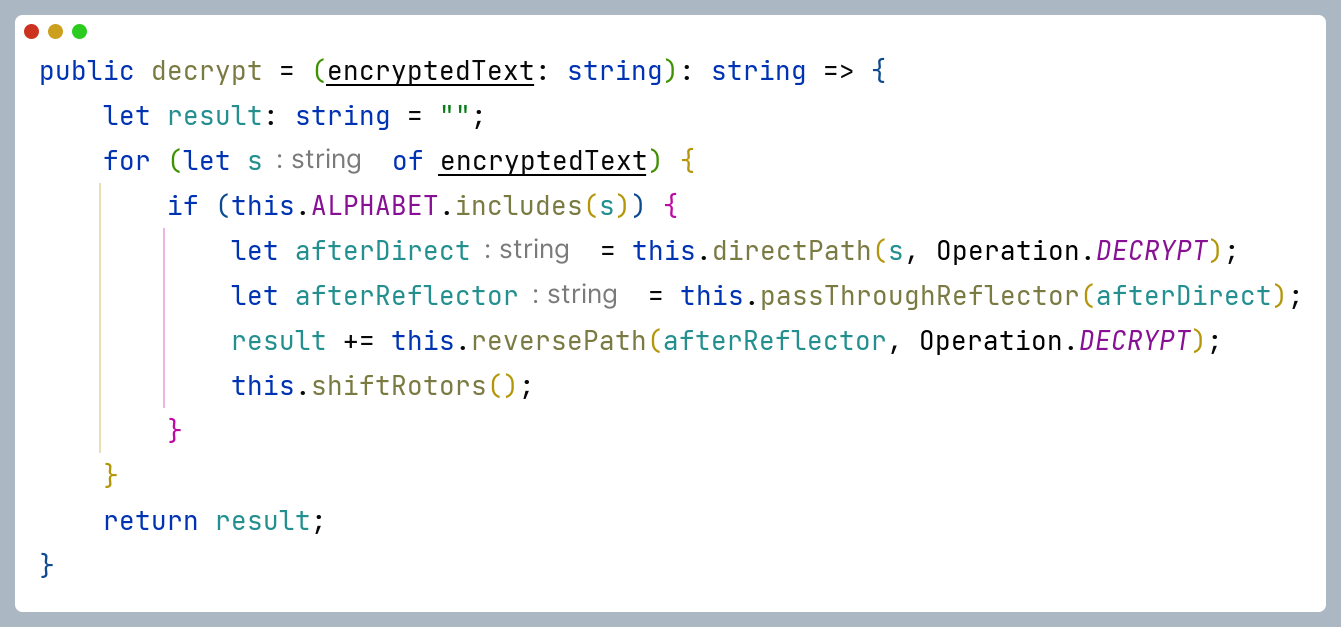


Рисунок 2.5 – Код метода расшифрования

Кроме того, класс Enigma позволяет устанавливать начальные положения роторов в своём конструкторе.

Пример зашифрования одного символа, если L – Beta, M – VIII, R – I, Re – B Dunn, Li-Mi-Ri = 3-1-3:

1. Шифруемый символ: r, исходный алфавит: abcdefghijklmnopqrstuvwxyz;
2. Ротор R в положении 3: mflgdqvzntowyhxuspaibrcjek. Положение символа r в исходном алфавите: 17. Производим замену r 🡪 a;
3. Ротор M в положении 1: kqhtlxocbjspdzramewniuygvf. Положение символа a в исходном алфавите: 0. Производим замену a 🡪 k;
4. Ротор L в положении 3: yjvcnixwpbqmdrtakzgfuhosle. Положение символа k в исходном алфавите: 10. Производим замену k 🡪 m;
5. Далее символ m проходит через рефлектор. Производим замену: m 🡪 p;
6. Обратный ход через ротор L. Положение символа p в алфавите ротора L: 10. Производим замену p 🡪 n;
7. Обратный ход через ротор M. Положение символа n в алфавите ротора M: 20. Производим замену n 🡪 v;
8. Обратный ход через ротор R. Положение символа v в алфавите ротора R: 8. Производим последнюю замену v 🡪 l.
9. Далее роторы смещаются и начинается шифрование следующего символа.

Результат работы приложения для роторов в позиции 3-1-3 приведен на рисунке 2.6.

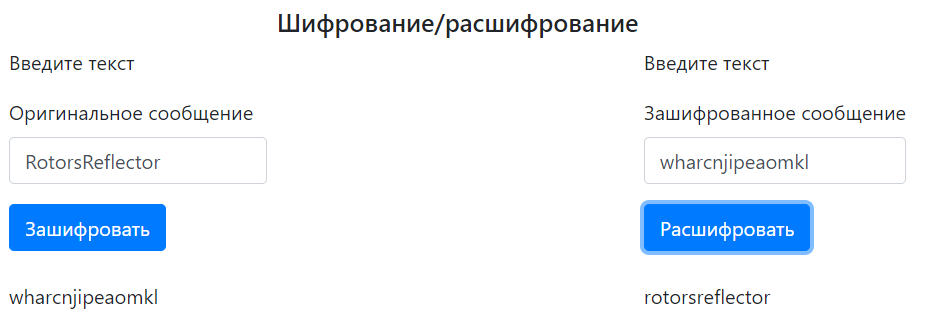


Рисунок 2.6 – Результат шифрования и дешифрования текста

Далее, нужно было сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений. Гистограмма частот появления символов исходного сообщения приведена на рисунке 2.7.

Рисунок 2.7 – Гистограмма частот появления символов исходного сообщения

Гистограмма частот появления символов зашифрованного сообщения приведена на рисунке 2.8.

Рисунок 2.8 – Гистограмма частот появления символов зашифрованного сообщения

Можно заметить, что частоты появления не совпадают, что значительно увеличивает криптостойкость шифра машины «Энигма».

**Вывод:** в ходе выполнения лабораторной работы были изучены приницпы функционирования машин семейства «Энигма». Также было разработано приложение для реализации зашифрования и расшифрования с помощью симулятора машины «Энигма». Было выполнено исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.