Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Изучение устройства и функциональных особенностей шифровальной машины «Энигма»

Студент: Валдайцев А. Д.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

# Устройство шифровальной машины «Энигма»

Машина «Энигма» – это электромеханическое устройство шифрования. 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).

Общий принцип таков:

При каждом нажатии на клавишу самый правый ротор сдвигался на одну или несколько позиций, а остальные роторы сдвигались на одну или несколько позиций в случае, если ротор, расположенный справа, делал полный оборот.

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.

Идея заключается в том, чтобы добиться этих подстановок электрическими связями. Механические части двигались и, замыкая контакты, образовывали меняющийся электрический контур.

При нажатии на клавишу клавиатуры контур замыкается, ток проходит через созданную электрическую цепь и в результате включает одну из набора лампочек, отображающую искомую букву шифротекста (или расшифрованного сообщения).

# Зашифрование машиной «Энигма»

Для реализации зашифрования необходимо, во-первых, хранить в памяти следующие данные:

* подстановочные алфавиты, соответствующие каждому ротору;
* текущую позицию каждого ротора;
* общее количество смещений каждого ротора;
* количество полных оборотов роторов;
* шаги смещения каждого ротора.

Для имплементации хранения этих данных созданы следующие поля класса, представленные на рисунке 1.1.



Рисунок 1.1 – Поля для хранения данных

Также через конструктор класса возможно задать стартовые позиции роторов (то есть количество символов, на сколько будет сдвинут каждый ротор). Позиции могут быть только в диапазоне от 0 до 25, так как в английском алфавите, используем для шифрования, 26 символов. При установке некорректных значений в конструктор класса будет возвращено исключение. Структура конструктора класса представлена на рисунке 1.2.

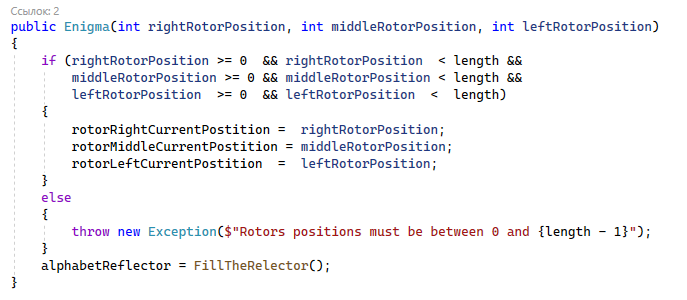


Рисунок 1.2 – Конструктор класса

Рассмотрим подробнее сам алгоритм зашифрования. Исходный открытый текст разбивается посимвольно и, если в английском алфавите присутствует такой символ, то производится зашифрование, иначе символ остается неизменным (например, знаки пунктуации не шифруются).

Далее символ шифруется правым ротором. Каждый ротор имеет собственную конфигурацию алфавита подстановки, которые были описаны ранее на рисунке 1.1. Для каждого ротора используется одинаковый алгоритм шифрования, предполагающий сдвиг на определенное количество позиций. Алгоритм зашифрования каждым ротором представлен на рисунке 1.3.

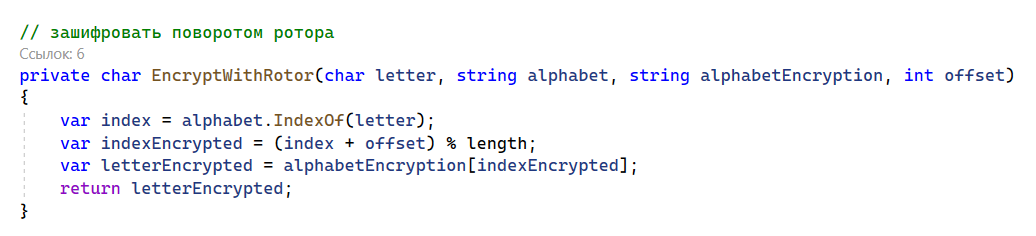


Рисунок 1.3 – Функция зашифрования ротором

Символ, который был получен при зашифровании правым ротором, передается в качестве входного параметра для среднего ротора. Аналогично, символ, зашифрованный средним ротором, шифруется после левым ротором. То есть, изначальный символ на данном этапе уже был зашифрован 3 раза.

Далее символ, полученный после зашифрования левым ротором, передается на рефлектор – устройство, которое также выполняет подстановку одного символа другим. Для реализации рефлектора используются пары символов, где каждый символ подставляется другим. Имплементация функции для зашифрования рефлектором представлена на рисунке 1.4.

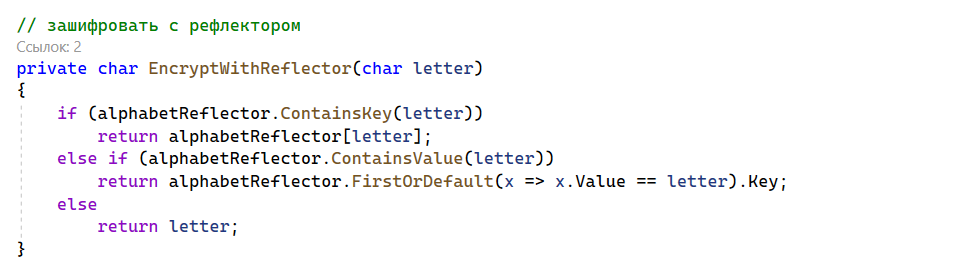


Рисунок 1.4 – Функция зашифрования рефлектором

После зашифрования рефлектором, символ исходного текста проходит те же самые роторы в обратном порядке. Выполняются еще 3 замены символа, и, учитывая замену в рефлекторе, символ будет заменён 7 раз.

Далее необходимо учесть повороты роторов. Правый ротор в конце шифрования каждого символа сдвигается на определённое количество символов, а средний и левый ротор будут сдвигаться только если расположенный правее ротор совершит полный оборот. Код для поворота роторов, а также код для функции зашифрования представлен на рисунке 1.5.

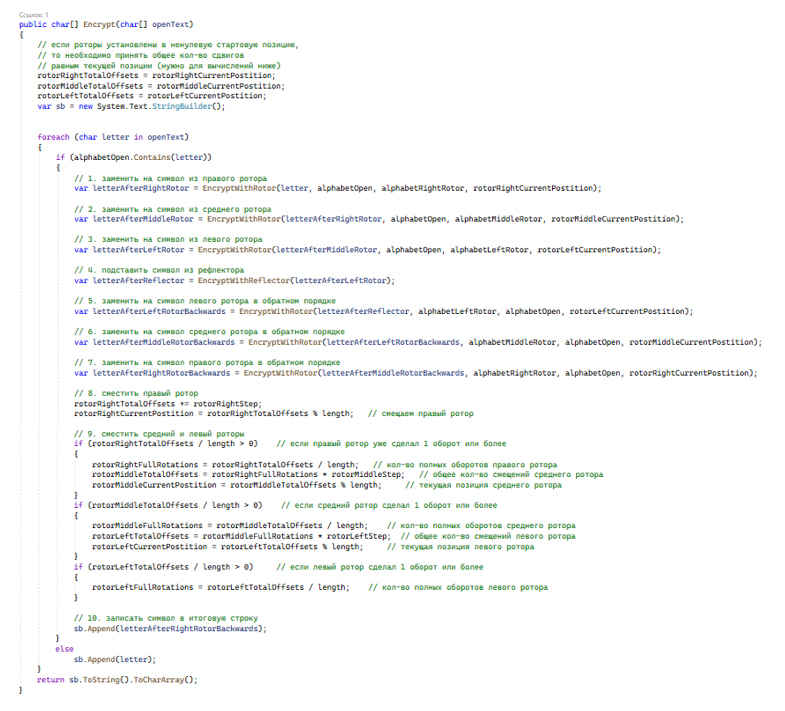


Рисунок 1.5 – Функция зашифрования машиной «Энигма»

# Расшифрование машиной «Энигма»

Для расшифрования необходимо установить роторы в такие же позиции, как и при зашифрования. Алгоритм аналогичен, кроме функции расшифрования ротором. Данная функция изображена на рисунке 1.6.

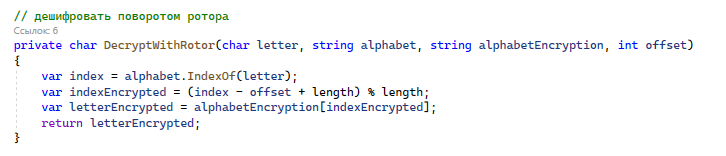


Рисунок 1.6 – Функция расшифрования с помощью ротора

# Криптостойкость машины «Энигма»

Для оценки криптостойкости проведем частотный анализ и сформируем таблицы частот появления символов в открытом тексте и в шифротексте. Данные графики представлены на рисунке 2.1.

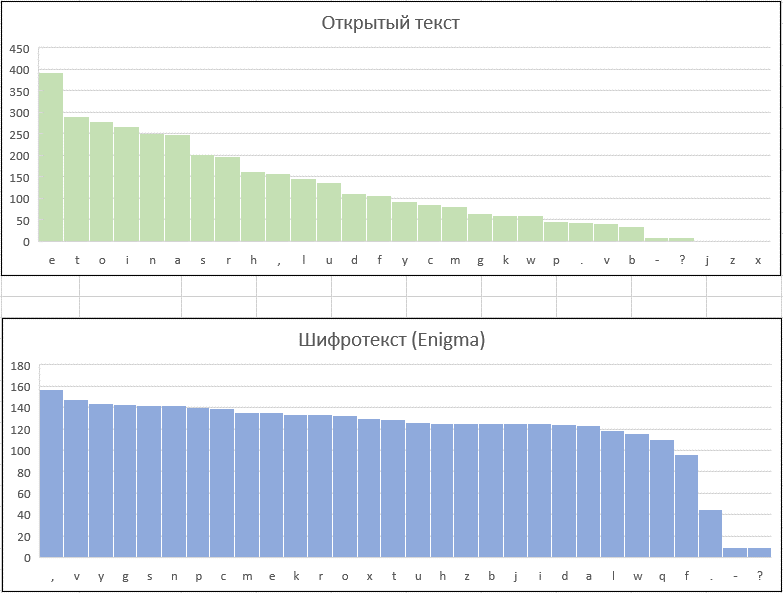


Рисунок 2.1 – Графики частот появления символов

Как видно из графиков, одним из важных преимуществ шифрования с помощью машины «Энигма» является то, что частоты появления символов являются примерно одинаковыми. Следовательно, частотный анализ не даст для криптоанализа больших результатов.

# Вывод

Машина «Энигма» получила широкое распространение во время Второй Мировой войны за счёт своей высокой криптостойкости. Она достигается за счёт того, что каждый символ шифруется 7 раз (в варианте с тремя роторами без коммутационной панели), причём при шифровании каждого символа получается новый символ, что также повышает криптостойкость.

В сравнении моего варианта реализации с реальной машиной «Энигма», мой вариант является немного менее криптостойким за счёт отсутствия коммутационной панели, которая добавляет от 0 до 2 замен каждого символа. Однако, шифровальная машина «Энигма» все так же является в разы более криптостойкой, чем рассмотренные ранее шифры.