МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №6**

**″Изучение устройства и функциональных особенностей шифровальной машины «Энигма»″**

Выполнила студентка 3 курса 5 группы Максимчикова Ю. С.

Проверила: Блинова Е. А.

Минск 2020

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

**Задачи**:

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочно-перестановочных шифров.
* Изучить структуру, принципы функционирования, реализацию процедур зашифрования сообщений в машинах семейства Энигма.
* Изучить и приобрести практические навыки выполнения криптопреобразований информации на платформе Энигма, реализованной в виде симуляторов.
* Получить практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе Энигма.
* Результаты выполнения лабораторной работы оформить в виде отчета проведенных исследованиях, методики выполнения практической части задания и оценки криптостойкости шифров.

В первом задании нужно было использовать симулятор Энигмы и произвести шифрование при различных настройках.

1. Роторы: VI, I, III; Рефлектор: B; стартовая позиция: AQL; исходное сообщение: MAXIMCHIKOVAYULIYASERGEEVNA; зашифрованное сообщение: rhizkyxhfwyoggilwkansndgcrj.
2. Роторы: VIII, III, VI; Рефлектор: C; стартовая позиция: DTO; исходное сообщение: MAXIMCHIKOVAYULIYASERGEEVNA; зашифрованное сообщение: tlfvbyylgennkhhwvfnudaixbir.
3. Роторы: VIII, II, VI; Рефлектор: B; стартовая позиция: DTO; исходное сообщение: MAXIMCHIKOVAYULIYASERGEEVNA; зашифрованное сообщение: xnueznfqipbdpfczixmyqvitzen.

Во втором задании необходимо было разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Типы роторов (L-M-R) и отражателя Re следовало выбрать в соответствии с вариантом. Для варианта 11 были заданы роторы (Beta, VIII, I) и отражатель B Dunn. С помощью разработанного приложения нужно было зашифровать сообщение из собственных фамилии, имени и отчества, применив не менее 5 вариантов начальных установок роторов.

Разработанное средство представляет собой обычное консольное приложение, позволяющее ввести начальную позицию роторов и текст, который будет зашифрован. После установки начальной позиции в консоль осуществляется вывод конфигураций роторов и отражателя. После выполнения операции в консоль выводится шифротекст. Также программа осуществляет подсчёт частот появления символов в исходном и зашифрованном текстах, выводя результаты в отдельные файлы.

**Разбор программного средства.** Константами заданы строки с алфавитом, символами, нанесёнными на каждый ротор и с парами букв отражателя. Константы представлены на рисунке 1.

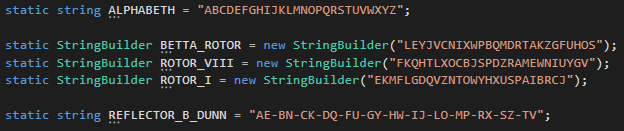


Рис. 1 – Значения роторов, отражателя и алфавит в виде констант

Установка роторов в начальную позицию, указанную пользователем, происходит в функции SetupRoters. Её программный код представлен на рисунке 2.

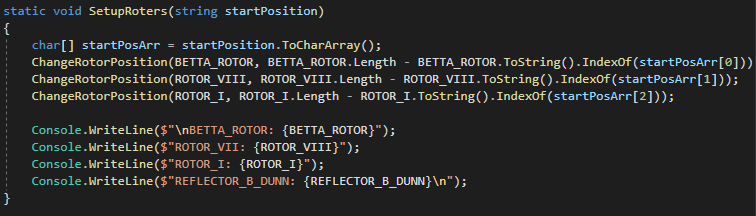


Рис. 2 – Функция, устанавливающая роторы в начальную позицию

Функция SetupRoters вызывает функцию ChangeRoutePosition, которая непосредственно и выполняет смену положения роторов. Её код представлен на рисунке 3.

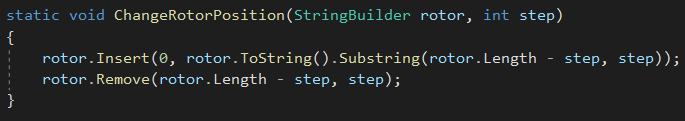


Рис. 3 – Функция, которая передвигает позицию указанного ротора на указанное количество шагов

На рисунке 4 представлена функция, имитирующая нажатие клавиши. Результатом её выполнения является зашифрованный символ.

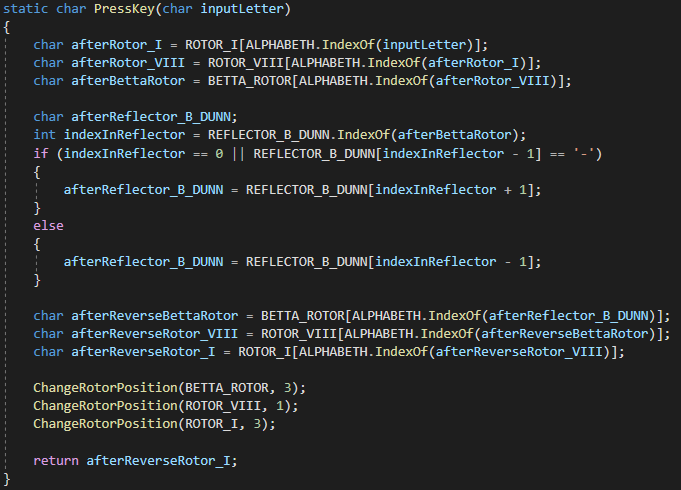


Рис. 4 – Функция, имитирующая нажатие клавиши

Также в программе ведётся подсчёт частоты символов. Его реализует функция CalculateFrequency. Её код представлен ниже на рисунке 5.



Рис. 5 – Функция для подсчёта частоты появления символов

Для тестирования разработанного приложения был использовано сообщение «MAXIMCHIKOVAYULIYASERGEEVNA». Результаты работы приложения с различными начальными установками роторов представлены на рисунке 6.

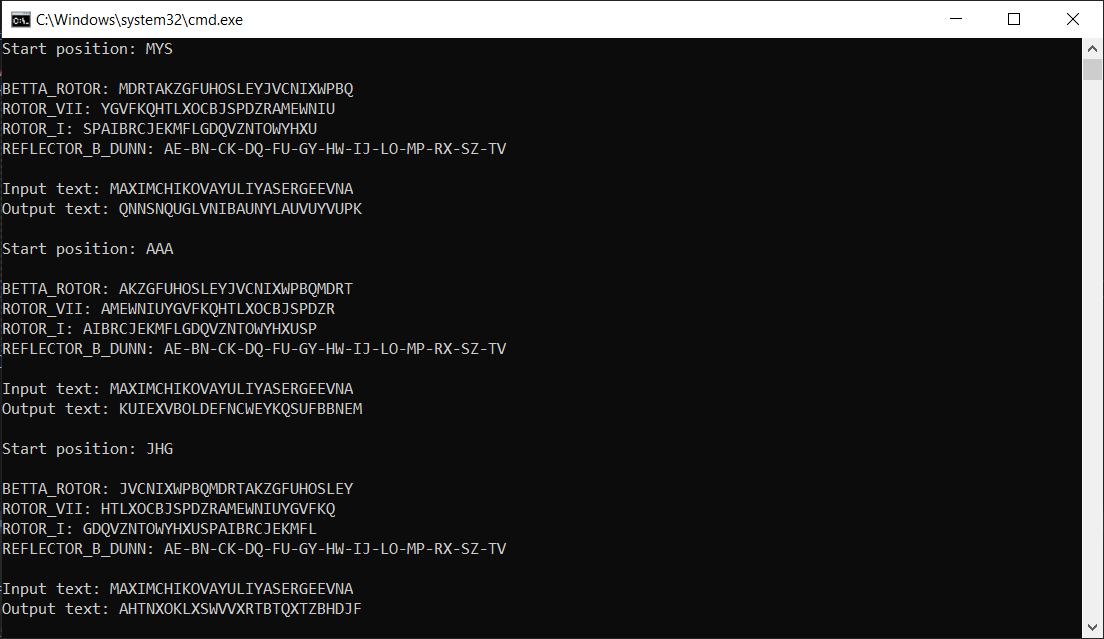


Рис. 6 – Результаты работы программного решения

Вывод: в результате данной лабораторной работы было разработано приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя.