МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Информационных систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Направление специальности 1-40 01 01 10 Программирование интернет-приложений

**ОТЧЁТ К ЛАБОРАТОРНОЙ РАБОТЕ №6:**

по дисциплине «Криптографические методы защиты информации»

Исполнитель

студентка 3 курса группы 5 Шкода Кристина Михайловна

(Ф.И.О.)

Руководитель работы преподаватель Савельева М. Г.

(учен. степень, звание, должность, подпись, Ф.И.О.)

Минск 2023

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

**Цель**: изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров (работа рассчитана на 4 часа аудиторных занятий).

**Задачи**:

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочно-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 отчета о проведенных исследованиях, методике выполнения практической части задания и оценке криптостойкости шифров.

**Ход работы**

Приложение разработано на NodeJS.

Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Крайний правый столбец этой таблицы показывает, на какое число шагов (букв, *i*) перемещается соответствующий ротор при зашифровании одного (текущего) символа; число 0 означает перемещение соответствующего ротора на один шаг при условии, что расположенный правее ротор совершит один оборот.

При разваботке моего приложения я использовала значения в ссответствии с 13 вариантом.

Значения левого, среднего и правого ротера соответствуют типам 6 ,4, 2 и были внесены в многомерный массив. Это представлено на рисунке 1.

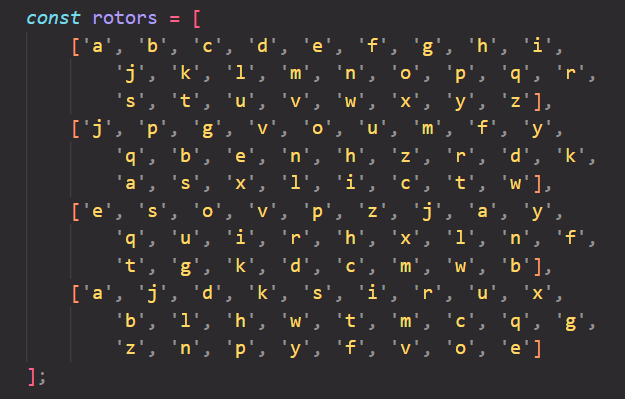


Рисунок 1 — Роторы

В данном приложении я использовала отображатель *Re* типа В. Данные по данному типу были занесены в переменную как объект. Отображатель и количества сдвигов представлены на рисунке 2.

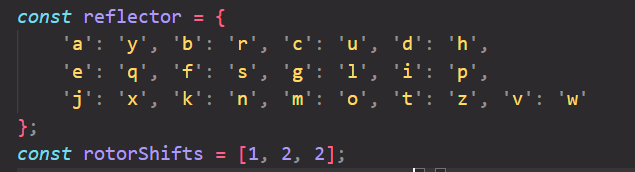


Рисунок 2 — Отображатель и сдвиги

Функция реализующая метод шифра по продемонстрирована на рисунке 3.



Рисунок 3 — Функция-шифратор

Еще есть функция сдвига позиции роутера при каждом наборе символе на определенную позицию. Эта функция называется ShiftRotors и она показана на рисунке 4.



Рисунок 4 — Функция сдвига позиции роутера

Так же в моем коде есть функция установки последовательности роторов при шифровании, которая представлена на рисунке 5.

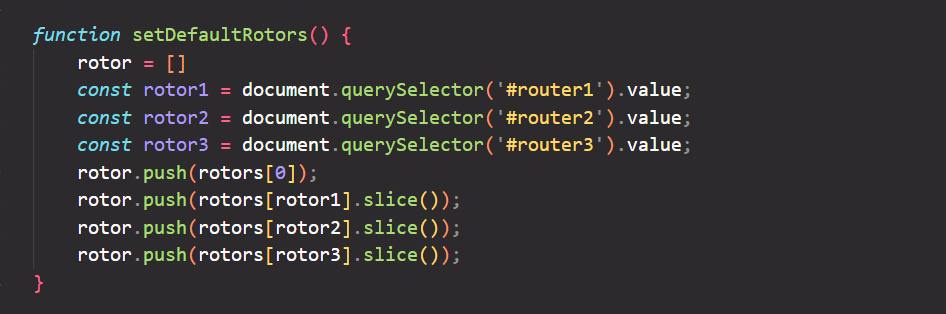


Рисунок 5 — Функция для установки последовательности роторов

Процесс использования приложения для шифрования и дешифрования представлен на рисунке 6 и 7 соответственно.

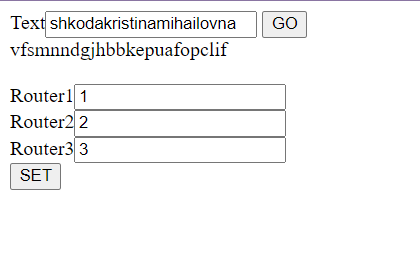


Рисунок 6 — Шифрование

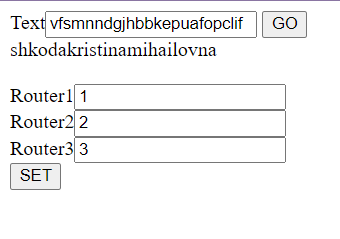


Рисунок 7 — Дешифрование

С учетом существования 10 возможных роторов, чтобы выбрать 3 ротора из возможных 10, существует 720 комбинаций 10\*9\*8 = 720.

Каждый ротор (его внутренняя проводка) может быть установлен в любом из 26 положений. Следовательно, с 3 роторами имеется 17 576 различных положений ротора 26\*26\*26 = 17 576.

Количество различных перестановок рефлекторов: всего имеется 26 букв, нам не важно, в каком порядке идут эти 13 пар, а также для каждой пары обратная пара будет той же парой («AB» = «BA»), поэтому число всех возможных перестановок 26 букв в рефлекторе будет равно: 26! / (13! \* 2^13)= = 64 764 752 532 480 000 / 8 192 = 7 905 853 580 625.

Таким образом, практически рассматриваемая версия «Энигмы» может быть настроена на 21 557 568 614 400 различных состояний 720 \* 17 576 \*   
\* 7 905 853 580 625 = 100 046 363 423 806 800 000 ~ 1e20.

Вывод: проделав данную лабораторную работу, я разобралась, как работает шифровальная машина «Энигма», из чего она состоит. Так же, сравнив ее с другими перестановочными шифрами, можно утверждать, что она обладает более высокой криптостойкостью.