Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Изучение устройства и функциональных особенностей**

**шифровальной машины «Энигма»**

Студент: Гвоздовский К.В.

ФИТ 3 курс 6 группа

Преподаватель:

Нистюк Ольга Александровна

1. **Цель работы**

Изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров.

1. **Задание**
2. Ознакомиться с функционалом хотя бы одного симулятора Энигмы.
3. Произвести зашифрование сообщения (собственные имя, отчество, фамилия) при 8-10 различных настройках машины-симулятора. Оценить частотные свойства символов в шифртекстах и сравнить этот параметр с частотными свойствами символов для исходного текста.
4. Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. С помощью разработанного приложения зашифровать сообщение в соответствии с п.1 практического задания, применив не менее 5 вариантов начальных установок роторов.
5. Оценить криптостойкость вашего варианта машины.
6. **Ход работы**

Ознакомился с функционалом симулятора «Энигмы». Произвёл зашифрование сообщения (собственное ФИО) при различных настройках машины-симулятора.

На сайте <https://piotte13.github.io/enigma-cipher/> присутствует возможность настройки машины «Энигма» с помощью 8 роторов и 2 рефлекторов. Результат шифрования собственного ФИО представлен на рисунке 3.1

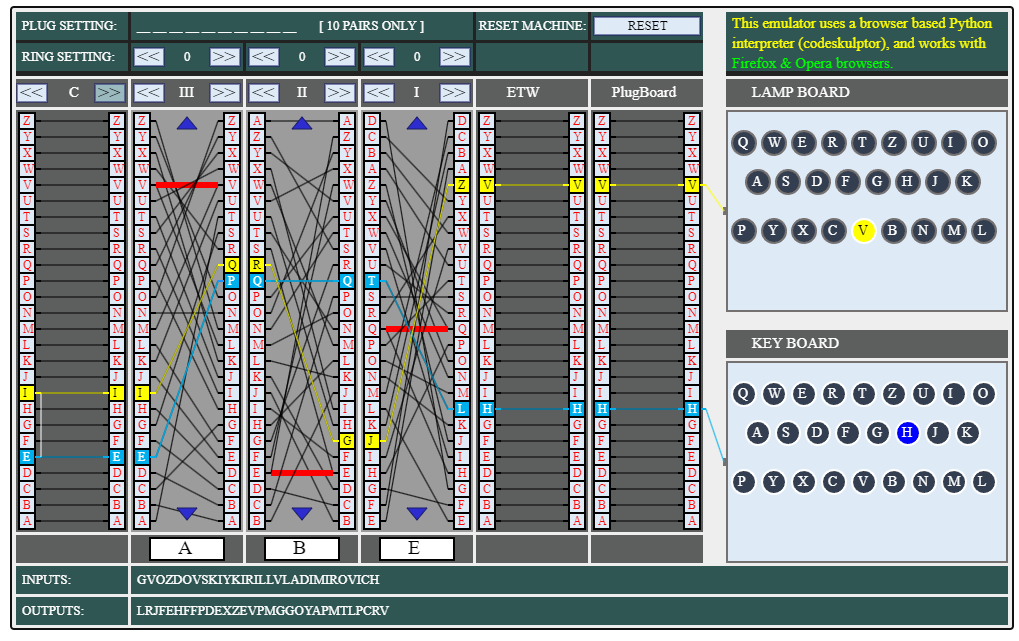
****

Рисунок 3.1 — Результат шифрования собственного ФИО на сайте <https://piotte13.github.io/enigma-cipher/>

Машина Энигма — это электромеханическое устройство, используемое для шифрования и дешифрования сообщений. Она использует несколько роторов, которые поворачиваются при каждом нажатии клавиши на клавиатуре. При повороте ротора, сигнал проходит через шифровальный элемент (например, перестановочную таблицу) и затем возвращается обратно через ротор и другие шифровальные элементы, проходя через каждый ротор на своем пути. Каждый ротор имеет свой набор проводников, называемый «коммутационной таблицей», которые перемешивают сигнал при каждом проходе.

В машине Энигма также используется «рефлектор», который направляет сигналы обратно через все роторы и шифровальные элементы в обратном порядке, создавая «обратный поток». Это создает эффект повторного шифрования, который повышает уровень защиты сообщения.

Машина Энигма имеет несколько настроек, которые могут быть изменены, чтобы изменить алгоритм шифрования. Например, можно изменить порядок роторов или коммутационных таблиц, а также количество и расположение роторов. Это делает машину Энигма очень трудной для взлома.

Код разработанного приложения реализуют функции enigma и rotorShift, который представляет собой шифровальную машину Энигма. Функция enigma принимает текущие позиции трех роторов, сообщение для шифрования. В функции настройки роторов и рефлектора. Также содержится функция rotorShift(), которая принимает на вход массив символов и возвращает символ после вращения ротора. Вот как работает алгоритм с помощью данных функций:

1. Создаются новые экземпляры роторов, инициализированные текущими позициями трех роторов.
2. Для каждого символа из строки message: если символ содержится в алфавите alphabet, то он передается через три ротора и рефлектор, после чего проходит через три ротора в обратном порядке и добавляется в результат. Если символ не содержится в алфавите alphabet, то он добавляется в результат без изменений.
3. После обработки каждого символа происходит проверка, нужно ли сдвинуть роторы. Если позиция самого левого ротора posL равна 0, то происходит проверка, достиг ли ротор rotorM конечной позиции, и если да, то он сдвигается на одну позицию вправо. Затем сдвигается ротор rotorR, а затем сдвигается ротор rotorM. Если позиция центрального ротора posM равна 0, то происходит проверка, достиг ли ротор rotorR конечной позиции, и если да, то он сдвигается на позицию, а ротор rotorM сдвигается на одну позицию. Затем роторы rotorR и rotorM сдвигаются на posL позиций влево.

Код этого алгоритма представлен на рисунках 3.1 и 3.2



Рисунок 3.1 – Функция enigma, реализующая шифровальную машину Энигма

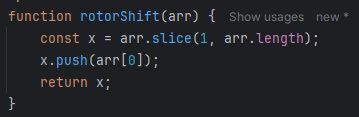


Рисунок 3.2 – Функция rotorShift, реализующая шифровальную машину Энигма

Далее, оценим криптостойкость машины Энигма с типом отражателя B Dunn, роторами III, VII, I.

Чтобы оценить криптостойкость шифра, нужно учитывать все возможные настройки машины. Для этого необходимо рассмотреть следующие свойства Энигмы:

* выбор и порядок роторов,
* разводку (коммутацию) роторов,
* настройку колец на каждом из роторов,
* начальное положение роторов в начале сообщения,
* отражатель,
* настройки коммутационной панели.

Чтобы выбрать 2 ротора из возможных 3, существует 6 комбинаций (3 ⋅ 2 ⋅ 1). Каждый ротор (его внутренняя проводка) может быть установлен в любом из 26 положений. Следовательно, с 3 роторами имеется 17576 различных положений ротора (26 ⋅ 26 ⋅ 26). Кольцо на каждом роторе содержит маркировку ротора и выемку, которая влияет на шаг перемещения расположенного левее ротора. Каждое кольцо может быть установлено в любом из 26 положений. Поскольку слева от третьего (наиболее левого) ротора нет ротора, на расчет влияют только кольца самого правого и среднего ротора. Это дает 676 комбинаций колец (26 ⋅ 26).

Получаем: 6 ⋅ 17576 ⋅ 676 = 71288256. В экспоненциальной форме записи 7.13 ⋅ 107 . Таким образом, практически рассматриваемая версия Энигмы (три ротора с выбором из 3 роторов, отражатель В Dunn) может быть настроена на 7.13 ⋅ 107 различных состояний, что сопоставимо с 26 – битным криптографическим ключом.

Алгоритм шифрования одной буквы G (при настройках роторов III, VII, I в 0,0,0):

* + - 1. Берём на вход букву G. Она поступает на левый ротор III и будет шифроваться в букву С.
      2. На средний ротор VII поступает буква C и шифруется в букву J.
      3. На правый ротор I поступает буква J и шифруется в букву Z.
      4. Буква Z поступает на рефлектор B Dunn и ставится в соответствие букве S.
      5. Буква S поступает на правый ротор I и шифруется в букву S.
      6. Буква S поступает на средний ротор VII и шифруется в букву K.
      7. Буква K поступает на левый ротор III и шифруется в букву U.
      8. На выходе буква G преобразуется в букву U.

**Вывод**

В ходе лабораторной работы были изучены и приобретены практические навыки разработки и использования приложений для реализации перестановочных шифров.

Также было разработано авторское приложение в соответствии с целью лабораторной работы и была оценена криптостойкость шифра для разработанной машины Энигма.