МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6 НА ТЕМУ:**

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

Выполнил студент 3 курса 6 группы

Подобед Владислав Георгиевич

Минск 2024

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

**Теоретические сведения**

**Машина «Энигма»** – это *электромеханическое* устройство.

Как и другие роторные машины, «Энигма» состоит из комбинации механических и электрических подсистем.

**Механическая часть:**

– клавиатура;

– набор вращающихся дисков – роторов (расположены вдоль вала);

– ступенчатый механизм

– скользящие контакты (для соединения роторов)

**Электрическая часть:**

– электрическая схема (соединяет клавиатуру, коммуникационную панель, лампочки, роторы)

5 основных блоков «Энигма»:

– панель механических клавиш;

– трёх (или более) роторных дисков, каждый имеет контакты по сторонам

– рефлекторы;

– коммутационные панели;

– панель в виде электрических лампочек (индикатор выходной буквы в процессе шифрования)

**Общий принцип механизма машины «Энигма»:**

– 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.

– при нажатии на клавишу, контру замыкается, включается одна из набора лампочек, показывающая искомую букву шифртекста

Идея А. Шербиуса состояла в том, чтобы добиться этих подстановок электрическими связями.

**Алгоритм зашифрования сообщения:**

1) Установка начальной позиции роторов согласно текущей кодовой таблицу (коду дня), например, *WZA*

2) Выбрать случайный ключ сообщения, например, *SXT*

3) Зашифровать ключ сообщения *SXT*. Например, получилось *UHL*

4) Оператор ставит ключ сообщения *SXT* как начальную позицию роторов и зашифровал собственно сообщение

5) Отправляет стартовую позицию *WZA* и зашифрованный ключ *UHL* вместе с сообщением

**Алгоритм расшифровки сообщения:**

1) Роторы ставим в соответствии с первой треграммой *WZA*

2) Расшифровываем вторую треграмму *UHL* –> извлекаем исходный ключ *SXT*

3) Используем исходный ключ как стартовую позицию для расшифрования текста

«Энигма» строится на основе подстановочных шифров, подобных шифру Цезаря, в котором, как известно, ключ сообщения, который должен знать получатель, – это просто смещение между двумя алфавитами. Принято считать, что в основе шифра «Энигмы» лежит динамический шифр Цезаря.

Рассмотрим трехроторную модель «Энигмы». Положим, что символом *В* обозначаются операции с использованием коммутационной панели, соответственно, символы *Re* – отражателя, а *L*, *M* и *R* обозначают действия левых, средних и правых роторов соответственно. Тогда процесс зашифрования символа *m* c использованием некоторой ключевой информации *K* формально можно записать в следующем виде:



**Практическое задание**

1. Ознакомиться с функционалом хотя бы одного (по согласованию с преподавателем) симулятора «Энигмы». 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.

Сайт <https://piotte13.github.io/enigma-cipher/> позволяет настраивать машину с помощью 8 моделей роторов и 2 моделей рефлекторов, а так же графически отображает каждый шаг шифрования букв. Пример шифрования собственного ФИО при использовании роторов I, II, III и рефлектора *B* представлен на рисунке 1.

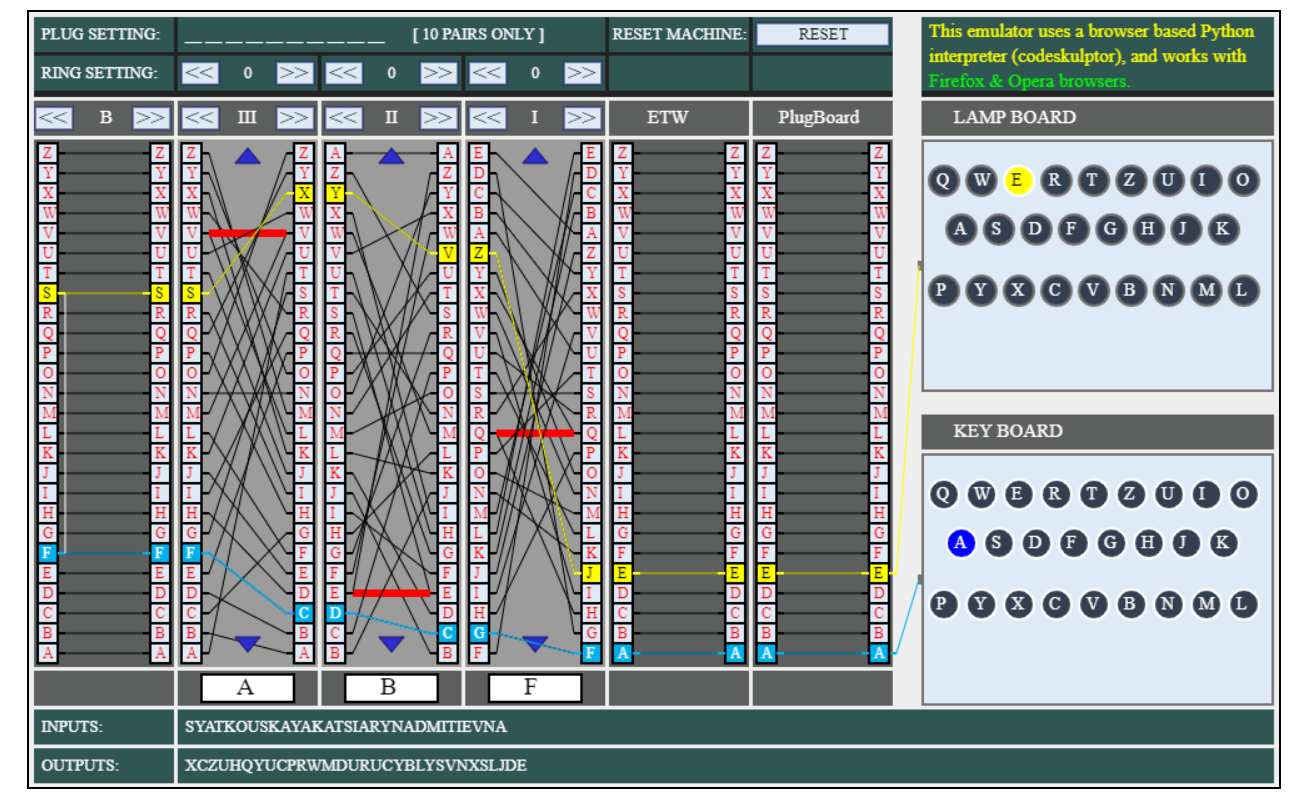


Рисунок 1 – Шифрование ФИО с использованием эмулятора

1. Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Типы роторов (*L – M – R*) и отражателя *Re* следует выбрать из рис. 4.5 и 4.6 в соответствии со своим вариантом, представленным в таблице. 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.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вариант | *L* | *M* | *R* | *Re* | *LiMiRi* |
| 9 | VIII | II | IV | B | 1-0-1 |

С помощью разработанного приложения зашифровать сообщение в соответствии с п. 1 практического задания, применив не менее 5 вариантов начальных установок роторов.

Оценить криптостойкость вашего варианта машины.

Распишем процесс шифрования на примере шифрования буквы «*S*».

Указывая фактическую разводку ротора, это значит, что правый ротор *R* (V) производит подстановку в соответствии с переставленными буквами исходного алфавита, т.е. буква «*S*» будет заменена буквой «*T*»:

ABCDEFGHIJKLMNOPQR **S** TUVWXYZ

ESOVPZJAYQUIRHXLNF **T** GKDCMWB

Центральный ротор (*М*) или Gamma заменяет букву «T» на «N»:

ABCDEFGHIJKLMNOPQRS **T** UVWXYZ

AJDKSIRUXBLHWTMCQG **N** PYFVOE

Левый ротор (*L*) или III соответственно букву «*N*» на «D»:

ABCDEFGHIJKLM **N** OPQRSTUVWXY Z

FKQHTLXOCBJSP **D** ZRAMEWNIUYG V

Используя *B* рефлектор, осуществляем подстановку с «*D*» на «*H*»:

(AY) (BR) (CU) (DH) (EQ) (FS) (GL) (IP) (JX) (KN) (MO) (TZ) (VW)

Ток теперь проходит обратный путь через три ротора в последовательности *L* → *M* → *R*. Эффект преобразования левого ротора (обратный):

FKQ **H** TLXOCBJSPDZRAMEWNIUYGV

ABC **D** EFGHIJKLMNOPQRSTUVWXYZ

соответственно – среднего ротора (обратный):

AJ **D** KSIRUXBLHWTMCQGZNPYFVOE

AB **C** DEFGHIJKLMNOPQRSTUVWXYZ

и, наконец, правого ротора (обратный):

ESOVPZJAYQUIRHXLNFTGKD **C** MWB

ABCDEFGHIJKLMNOPQRSTUV **W** XYZ

После всех подстановок буква «S» будет зашифрована буквой «W».

При обратных (слева-направо) перестановках (левый ротор-средний ротор-правый ротор) входной символ располагается в нижней строке (для каждого ротора), выходной – в верхней.

По такому же принципу осуществляются и остальные подстановки в обратной петле.

Код представлен на листинге 1.

|  |
| --- |
| def enigma(message : str, left\_rotor : str, middle\_rotor : str, right\_rotor : str) -> str:      res = ''      for character in message:          letter = right\_rotor[alphabet.index(character)]          letter = middle\_rotor[alphabet.index(letter)]          letter = left\_rotor[alphabet.index(letter)]          letter = reflector[letter]          letter = alphabet[left\_rotor.index(letter)]          letter = alphabet[middle\_rotor.index(letter)]          letter = alphabet[right\_rotor.index(letter)]          res += letter          left\_rotor = left\_rotor[1:] + left\_rotor[:1]          middle\_rotor = middle\_rotor[0:] + middle\_rotor[:0]          right\_rotor = right\_rotor[1:] + right\_rotor[:1]      return res |

Пример шифрования собственного ФИО без прокрутки роторов приведен на рисунке 3, с прокруткой – рисунок 4.

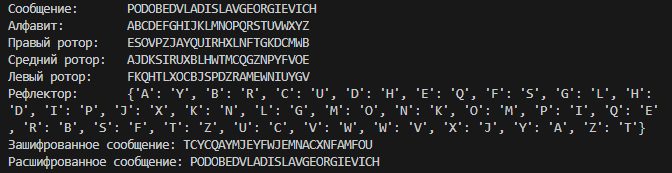
****

Рисунок 3 – Зашифрованное сообщение без прокрутки роторов

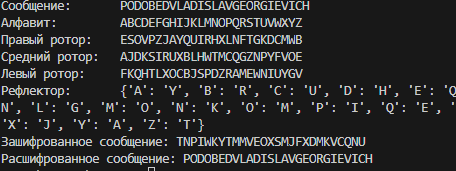


Рисунок 4 – Зашифрованное сообщение с прокруткой роторов

**Вывод:** в ходе лабораторной работы было изучено устройство и функциональные особенности шифровальной машины «Энигма». А также были приобретены практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе «Энигма».