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»**

Выполнила студентка 3 курса 4 группы

Сятковская Екатерина Дмитриевна

Минск 2023

**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.

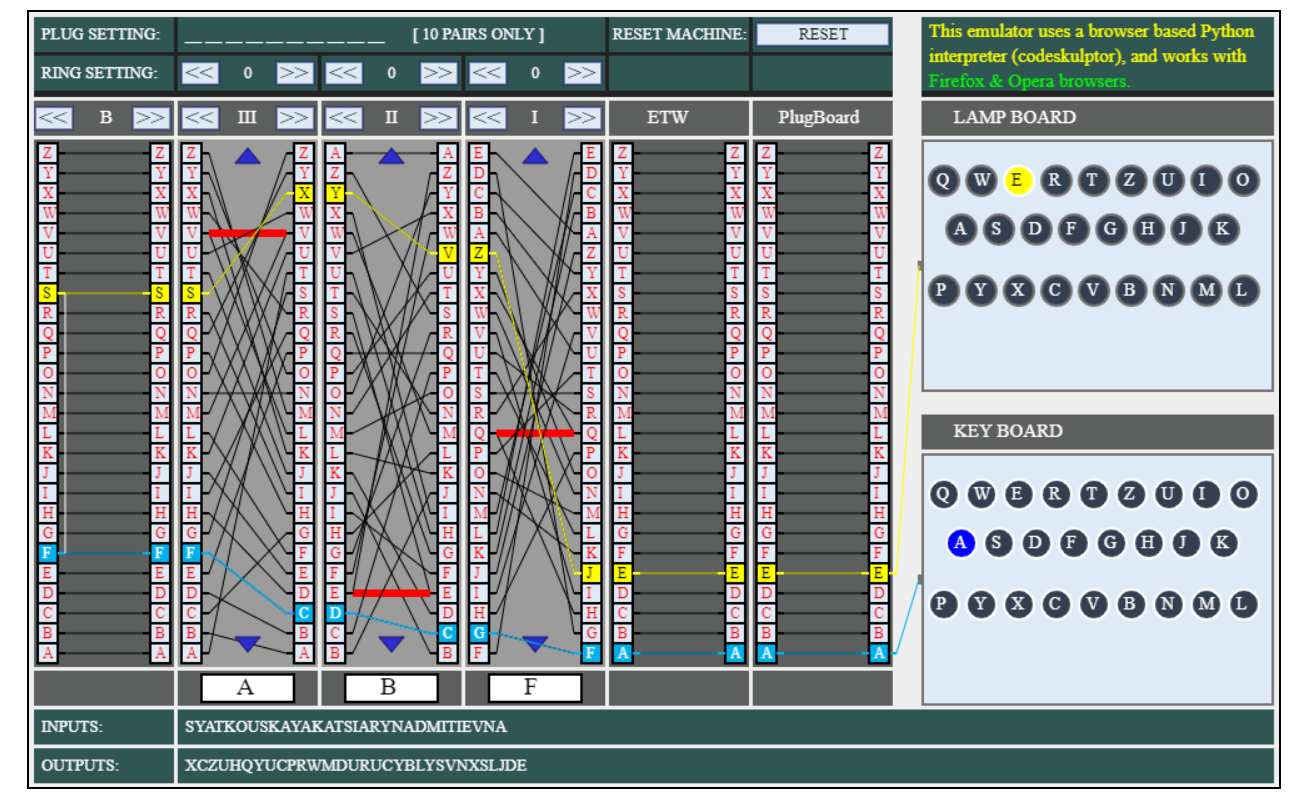


Рисунок 1 – Шифрование ФИО с использованием эмулятора

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* |
| 12 | III | Gamma | V | C Dunn | 1-1-2 |

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 «*M*»:

ABCDEFGHIJKLMNOPQR S TUVWXYZ

VZBRGITYUPSDNHLXAW M JQOFECK

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

ABCDEFGHIJKL M NOPQRSTUVWXYZ

FSOKANUERHMB T IYCWLQPZXVGJD

Левый ротор (*L*) или III соответственно букву «*T*» на «A»:

ABCDEFGHIJKLMNOPQRS T UVWXYZ

BDFHJLCPRTXVZNYEIWG A KMUSQO

Используя *C Dunn* рефлектор, осуществляем подстановку с «*A*» на «*R*»:

(AR) (BD) (CO) (EJ) (FN) (GT) (HK) (IV) (LM) (PW) (QZ) (SZ) (UY)

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

ABCDEFGHIJKLMNOPQRSTUVWXYZ

TAGBPCSDQEUFVNZHYIXJWLRKOM

соответственно – среднего ротора (обратный):

ABCDEFGHIJKLMNOPQRSTUVWXYZ

ELPZHAXJNYDRKFCTSIBMGWQVOU

и, наконец, правого ротора (обратный):

ABCDEFGHIJKLMNOPQRSTUVWXYZ

QCYLXWENFTZOSMVJUDKGIARPHB

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

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.

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

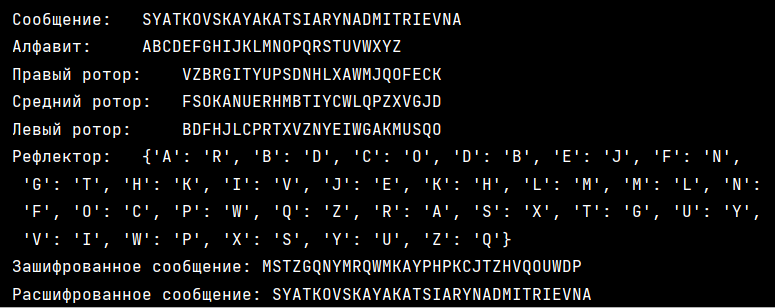


Рисунок 3 – Зашифрованное сообщение без прокрутки роторов

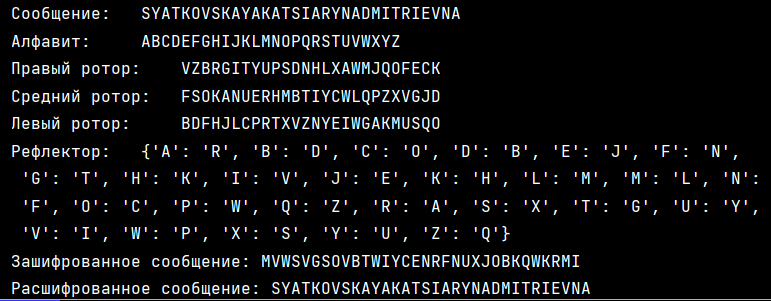
****

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».

**Контрольные вопросы:**

1. Дать пояснение к структуре шифровальных машин «Энигма».

«Энигма» состоит из 5 основных блоков:

* панели механических клавиш 1 (дают сигнал поворота роторных дисков);
* трех (или более) роторных дисков 2, каждый имеет контакты по сторонам, по 26 на каждую, которые коммутируют в случайном порядке; по окружности нанесены буквы латинского алфавита либо числа;
* рефлектора 3 (имеет контакты с крайним слева ротором);
* коммутационной панели 4 (служит для того, чтобы дополнительно менять местами электрические соединения (контакты) двух букв);
* панели в виде электрических лампочек 5; индикационная панель с лампочками служит индикатором выходной буквы в процессе шифрования

1. На основе каких шифров строится машина «Энигма»?

«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.

1. Дать характеристику криптостойкости шифровальной машины Энигма.

Преобразование «Энигмы» для каждой буквы может быть определено математически как результат подстановок.

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.

Немецкие криптологии полагали, что один ротор может быть подключен 4\*10^26 различными способами. Сочетание трех роторов и отражателя позволяет получить астрономические цифры возможных вариантов подстановок. Для союзников, которые знали конструкции роторов, число различных вариантов существенно уменьшалось.

Проблема криптоанализа шифров «Энигмы» была экстраординарной (с учетом электромеханических конструкций устройств для криптоанализа, применяемых в то время). Исчерпывающий поиск всех возможных 1,07 · 10^23 настроек был невозможен в 1940-х гг., а его сопоставимый 77-битный ключ огромен даже для современных электронных систем. Чтобы дать представление о размере этого числа, представим, что у нас есть 1,07 · 10^23 листов бумаги толщиной около 1 мм. Из этих листов можно сложить примерно 70 000 000 стопок бумаги, каждая из которых простирается от Земли до Солнца. Кроме того, 1,07 · 10^23 дюйма равно 288 500 световых лет.

1. Дать характеристику (с численными оценками) криптостойкости машины-симулятора на основе разработанного приложения.

Модель Энигмы имеет 3 различных ротора, пронумерованных римскими цифрами. При шифровании роторы можно располагать в любой последовательности, что для трех роторов дает 6 разных комбинаций. Помимо этого, каждый ротор может быть установлен в одной из 26 возможных стартовых позиций. Т.е. начальное положение роторов имеет всего 6\*26^3=105456 комбинаций.

Количество всех возможных соединений на коммутационной панели вычисляется по формуле n! /((n-2m)! m! 2^m), где n — количество букв алфавита, m — количество соединенных пар. Для 26 буква английского алфавита и 10 пар это составляет 150738274937250=2^47 различных комбинаций.

Таким образом базовая версия Энигмы с тремя роторами имеет солидное даже по современным меркам пространство ключей:

150738274937250\*105456=15,896,255,521,782,636,000≈2^64.

Если анализировать частоты (Рис. 5). Частоты символов в исходном тексте и зашифрованном сообщении сильно отличаются: некоторые символы вообще не появляются в шифре, а некоторые хоть и встречаются с такой же частотой, на находятся в совершенно других местах. Таким образом, криптостойкость разработанного симулятора такая же, как и у оригинальной машины.

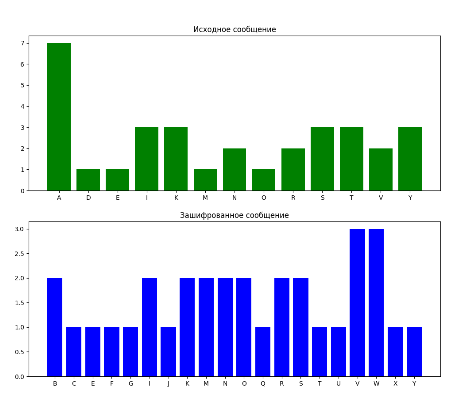


Рисунок 5 – Диаграмма частот сообщения собственного ФИО

1. Пояснить основные принципы расшифрования сообщений «Энигмы».

Процедура расшифрования шифртекстов предусматривала настройку отражателя, роторов и коммутационной панели машины в соответствии с таблицами (книгами) и использованными при зашифровании паролями.