МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3 НА ТЕМУ:

Исследование криптографических шифров на основе перестановки символов

Выполнила:

Студентка 3 курса 1 группы ФИТ

Шимчёнок Елизавета Константиновна

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

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочных шифров.

2. Ознакомиться с особенностями реализации и свойствами различных подстановочных шифров на основе готового программного средства (L\_LUX).

3. Разработать приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования.

4. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.

5. Оценить скорость зашифрования/расшифрования реализованных способов шифров.

6. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теоретические сведения**

Сущность перестановочного шифрования состоит в том, что исходный текст (из множества *М*) и зашифрованный текст (из множества *С*) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм перестановки.

Шифры перестановки относятся к классу *симметричных*. Элементами текста могут быть отдельные символы (самый распространенный случай), пары, тройки букв и т. д.

Классическими примерами перестановочных шифров являются анаграммы. Анаграмма (от греч. *ana* – снова и *gramma* – запись) – литературный прием, состоящий в перестановке букв (или звуков), что в результате дает другое слово или словосочетание, например: проездной – подрезной, листовка – вокалист, апельсин – спаниель.

В классической криптографии шифры перестановки делятся на два подкласса:

– шифры *простой*, или *одинарной*, *перестановки* – при зашифровании символы открытого текста *Мi* перемещаются с исходных

позиций в новые (в шифротексте *Сi*) один раз;

– шифры *сложной*, или *множественной*, *перестановки* – при

зашифровании символы открытого текста *Мi* перемещаются с исходных позиций в новые (в шифротексте *Сi*) несколько раз.

**Ход работы**

Для выполнения лабораторной работы были использованы данные варианта 2.

**Множественная перестановка**

Особенностью шифров данного подкласса *является минимум двукратная перестановка символов* шифруемого сообщения. В простейшем случае это может задаваться перемешиванием не только столбцов, но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного из них равна числу столбцов (мы используем имя «elizaveta»), другого – числу строк («shimchyonok»). К ключевой информацию мы можем относить также **способы вписывания сообщения** и **считывания отдельных символов** из текущего столбца матрицы.

Для реализации множественной перестановки необходимо сформировать таблицу (ключи фамилия и имя – «shimchyonok» и «elizaveta»). Далее записываем последовательно шифруемое сообщение в каждую ячейку. Способ вписывания: слева на право (Табл. 1).

Таблица 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ключи | E | L | I | Z | A |
| S | ч | ё | р | н | о |
| H | е |  | б | е | л |
| I | о | е |  | л | е |
| M | т | о |  | з | и |
| C | м | а |  | с | т |
| H | о | л | ь | к | о |

После по ключу сортируем в алфавитном порядке строки (Табл. 2).

Таблица 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ключи | E | L | I | Z | A |
| C | м | а |  | с | т |
| H | е |  | б | е | л |
| H | о | л | ь | к | о |
| I | о | е |  | л | е |
| M | т | о |  | з | и |
| S | ч | ё | р | н | о |

И в конце по второму ключу сортируем столбцы в алфавитном порядке (Табл. 3).

Таблица 3

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ключи | A | E | I | L | Z |
| C | т | м |  | а | с |
| H | л | е | б |  | е |
| H | о | о | ь | л | к |
| I | е | о |  | е | л |
| M | и | т |  | о | з |
| S | о | ч | р | ё | н |

Зашифрованное сообщение получается в результате считывания информации сверху вниз поколонно.

Сообщение до шифрования: «черное белое лето зима столько».

Сообщение после шифрования: «тлоеиомеоотч бь ра леоёсеклзн».

Проверка шифрования через приложение приведена на рисунке 1.

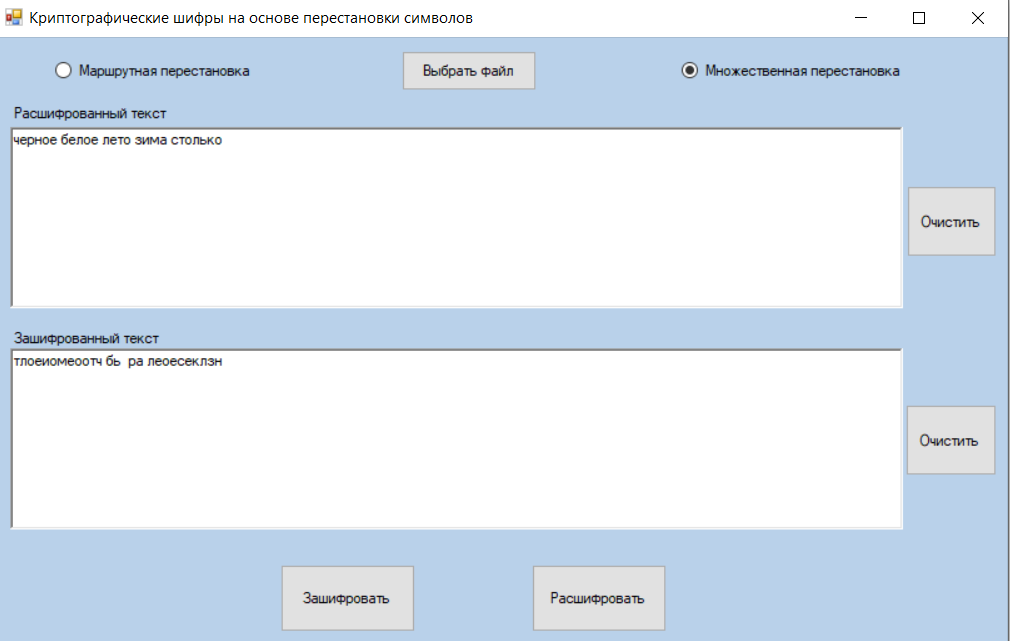


Рисунок 1 – Результат множественной перестановки

**Маршрутная перестановка**

Маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали, зигзагом, змейкой или каким-то другим способом. Такие способы шифрования несколько усложняют процесс, однако усиливают криптостойкость шифра.

По условию лабораторной маршрутная перестановка осуществляется по спирали (Рис. 2).

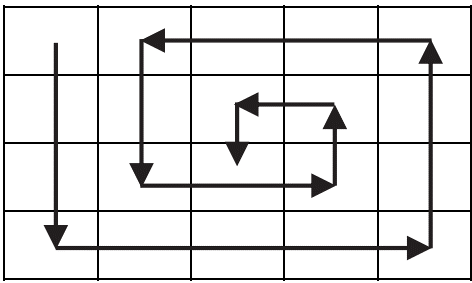


Рисунок 2 – Направление маршрутной перестановка по спирали

Результат шифрования большого текста посмотрим на Рисунке 3.

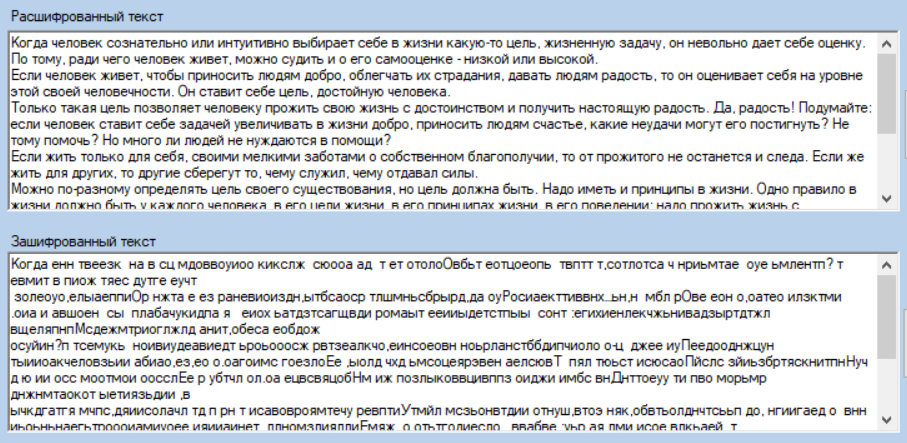


Рисунок 3 – Исходный и зашифрованный текст

Проверим работу программы на коротком предложении. За исходное сообщение возьмем «Никто не скажет, верно ты поступил или [нет](https://citaty.info/topic/net)». Для наглядности воспользуемся таблицей из 6 колонн (табл. 4), введем в нее наше сообщение слева направо. Считывать будем в соответствии с Рисунком 2.

Таблица 4

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Н | и | к | т | о |  |
| н | е |  | с | к | а |
| ж | е | т | , |  | в |
| е | р | н | о |  | т |
| ы |  | п | о | с | т |
| у | п | и | л |  | и |
| л | и |  | н | е | т |

Результат зашифровки: Никто авттитен илуыежне ск с лип рет,оопн.

Проверка результата шифротекста изображена на рисунке 4.

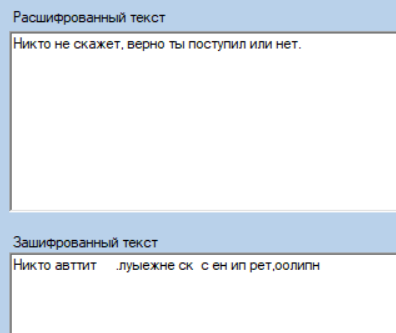


Рисунок 4 – Результат зашифровки короткого предложения

**Гистораммы алфавитов и оценка времени**

Далее приведем гистограммы частот появления символов для исходного и зашифрованного сообщений.

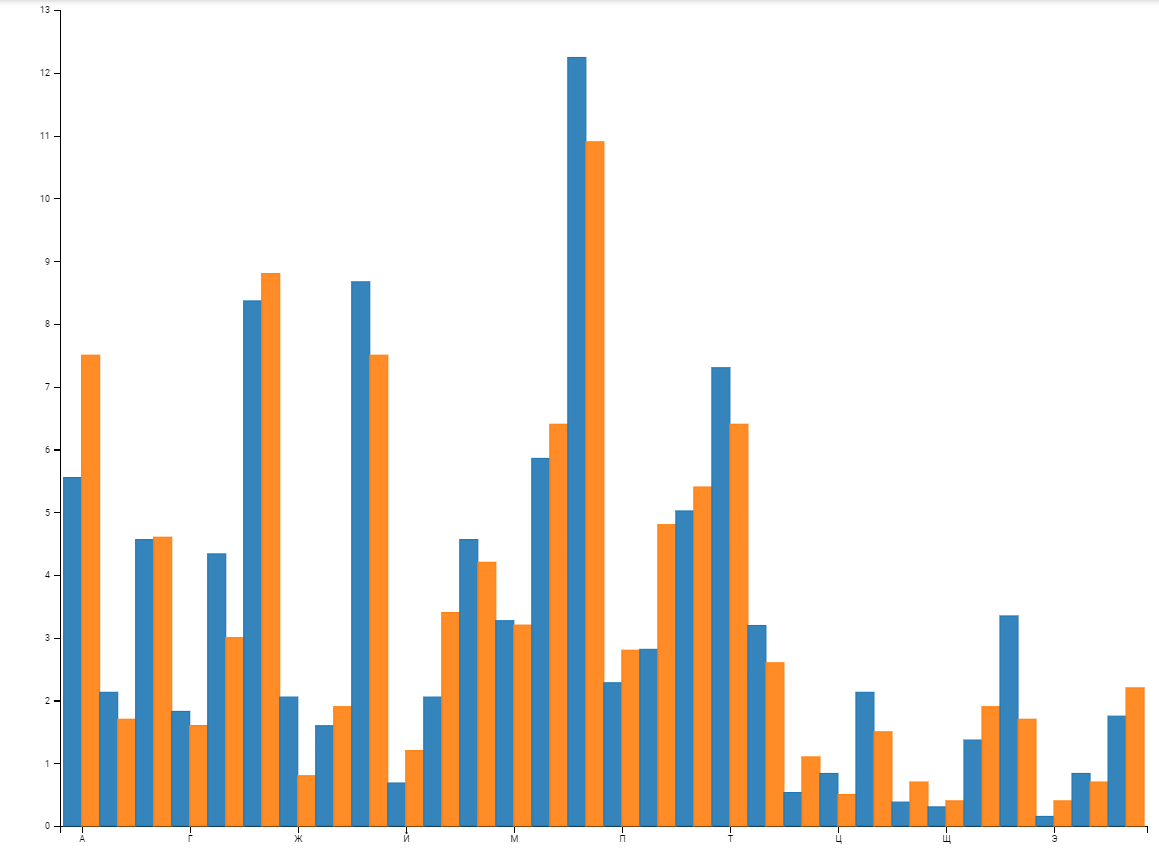
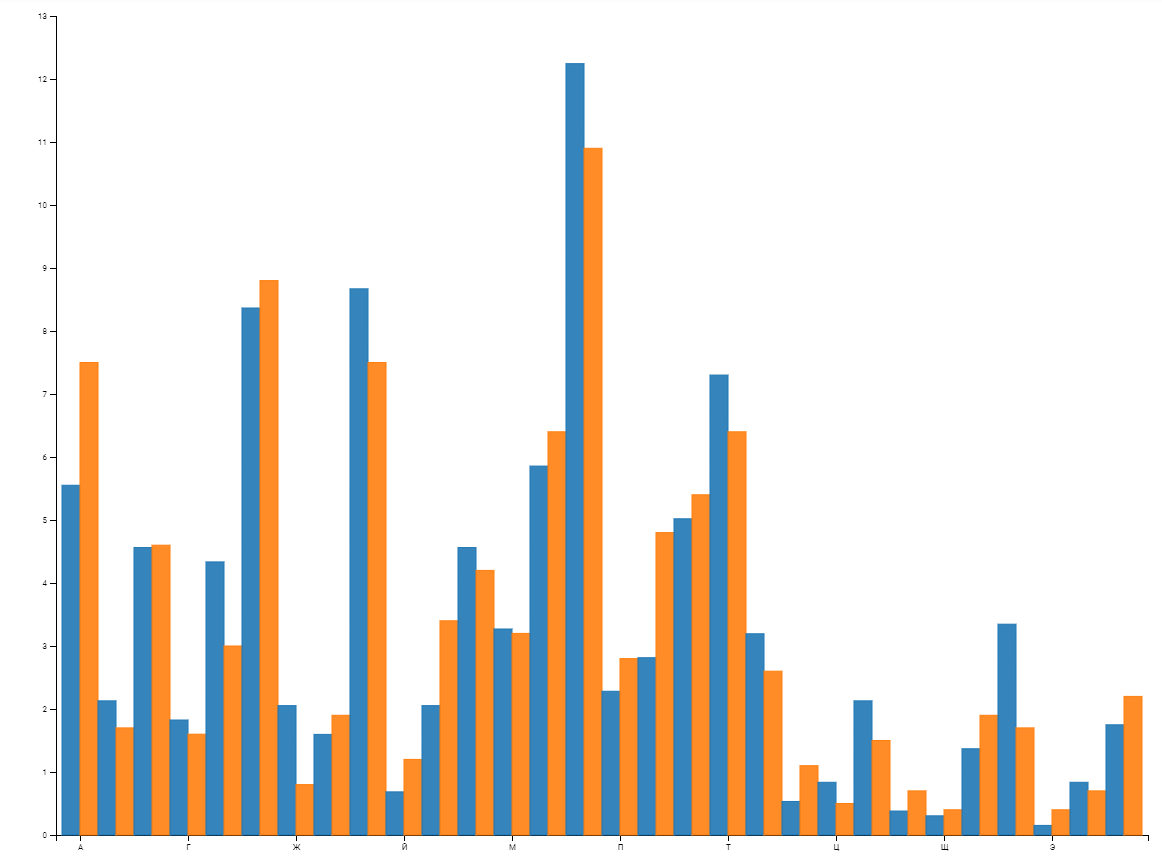
 

Рисунок 5 – Гистограмма исходного и шифро текстов

Гистограммы частот появления символов до и после шифрования изображены на рисунке 5. Проанализировав их, можно понять, что встречаемость символов во всех текстах остается одинаковой за счет того, что при шифровании символы лишь перемешиваются.

Оценка времени выполнения зашифровки и расшифровки текста, состоящего из 50 символов, была произведена (рис. 6, рис. 7) и проанализирована.



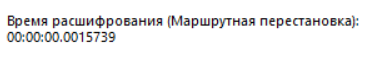


Рисунок 6 – Время шифрования/расшифрования с помощью маршрутной перестановки



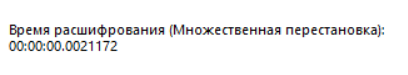


Рисунок 7 – Время шифрования/расшифрования с помощью множественной перестановки

Было выяснено, что шифрование методом множественной перестановки занимает немного больше времени, что связано с предварительной двойной перестановкой в матрице.

**Ответы на контрольные вопросы**

**1. В чем заключается основная идея криптографических преобразований на основе шифров перестановки?**

Сущность перестановочного шифрования состоит в том, что исходный текст и зашифрованный текст основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм перестановки.

**2. Привести классификационные признаки и дать сравнительную характеристику разновидностям перестановочных шифров.**

Простой перестановки/Простой блочной перестановки:при больших значениях n приходится работать с таблицами, состоящими из большого числа столбцов; для сообщений разной длины необходимо создавать разные таблицы перестановок – не очень удобен.

Маршрутной перестановки: геометрическая фигура, обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту (слева направо, сверху вниз или каким-либо иным образом) записывается открытый текст. Для получения шифрограммы нужно записать символы этого сообщения в иной последовательности, т. е. по иному маршруту.

Множественная перестановка: минимум двукратная перестановка символов шифруемого сообщения (перемещения не только столбцов, но и строк); использует 2 основных ключа (для строк и столбцов), а также к ключевой информацию мы можем относить также способы вписывания сообщения и считывания отдельных символов из текущего столбца матрицы.

**3. Сколько разновидностей шифров, подобных шифру Цезаря, можно составить для алфавитов русского и белорусского языков?**

Существует 4 разновидности шифра Цезаря, но так как мы можем комбинировать несколько шифров, необходимо найти сумму сочетаний, умноженную на 2, так как 2 алфавита:

**N=(i=14Ci4)\*2 = 4+6+4+1\*2 = 30**

**4. Охарактеризовать криптостойкость перестановочных и подстановочных шифров.**

Простой подстановочный шифр (моноалфавитный шифр) – это шифр, заменяющий каждый символ открытого текста соответствующим симоволом шифротекста. *Такие шифры взламываются без труда, поскольку не скрывают частоту использования различных символов в открытом тексте*.

Омофонический подстановочный шифр подобен простому подстановочному, но одному символу открытого текста может быть сопоставлен один из нескольких символов шифротекста. *Сложнее для вскрытия чем простые подст-ые, но не скрывают всех статистич. Свойств открытого текста. Без труда взламываются путем вскрытия с известным открытым текстом*.

Полиграмный (n-граммный) подстановочный шифр – шифрует блоки символов по группам. Подобный шифр использовался британцами во время Первой мировой войны.

Перестановочный шифр с множественной перестановкой является наиболее криптостойким, в связи с тем, что используется 2 ключа-слова и

**5. Привести примеры и дать характеристику перестановочным шифрам, не рассмотренным в материалах к данной лабораторной работе.**

Шифр «поворотная решётка»: изначально решётка Кардано представляла собой трафарет с отверстиями, в которые записывали буквы, слоги или слова сообщения. Затем трафарет убирали, а свободное место заполняли более или менее осмысленным текстом. Такой метод сокрытия информации относится к стеганографии.

**6. Имеются ли предпочтения в выборе размеров используемой таблицы для перестановочных шифров?**

Имеют. Например, при использовании метода простой перестановки, при больших значениях *n* приходится работать с таблицами, состоящими из большого числа столбцов, что неудобно. Если мы используем маршрутный метод, то для считывания информации определенным алгоритмом (зигзагом, по спирали), так же имеет значение, возьмём мы таблицу размерностью 2х5 или 5х5.

**7. Охарактеризовать основные методы взлома перестановочных шифров.**

Брутфорс – прямой перебор всех возможных вариантов перестановок.

Перебор ключей малой длины – перебор всех возможных ключей длиной до 9 символов.

Поиск восхождением к вершине – берётся часть шифртекста (называемая ключом), и оставшаяся часть расшифровывается с его помощью. Затем вычисляется коэффициент вероятности принадлежности расшифрованного текста к естественному языку. В ключе производятся какие-либо изменения (например, перестановка первых двух букв местами) и снова расшифровывается текст и вычисляется коэффициент. Так повторяется, пока коэффициент не перестанет изменяться.

Анализ на основе триграмм – можно попытаться вычислить примерный алгоритм перестановки, составляя наиболее часто встречающиеся в языке триграммы из символов сообщения.

**Вывод:** в ходе лабораторной работы были изучены криптографические шифры на основе перестановки, а также была рассмотрена программа, шифрующая и расшифровывающая текст из файла методом маршрутной и множественной перестановки. Затем рассмотрены гистограммы частот встречи символов текста и замерено время зашифровки/расшифровки сообщений.

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.

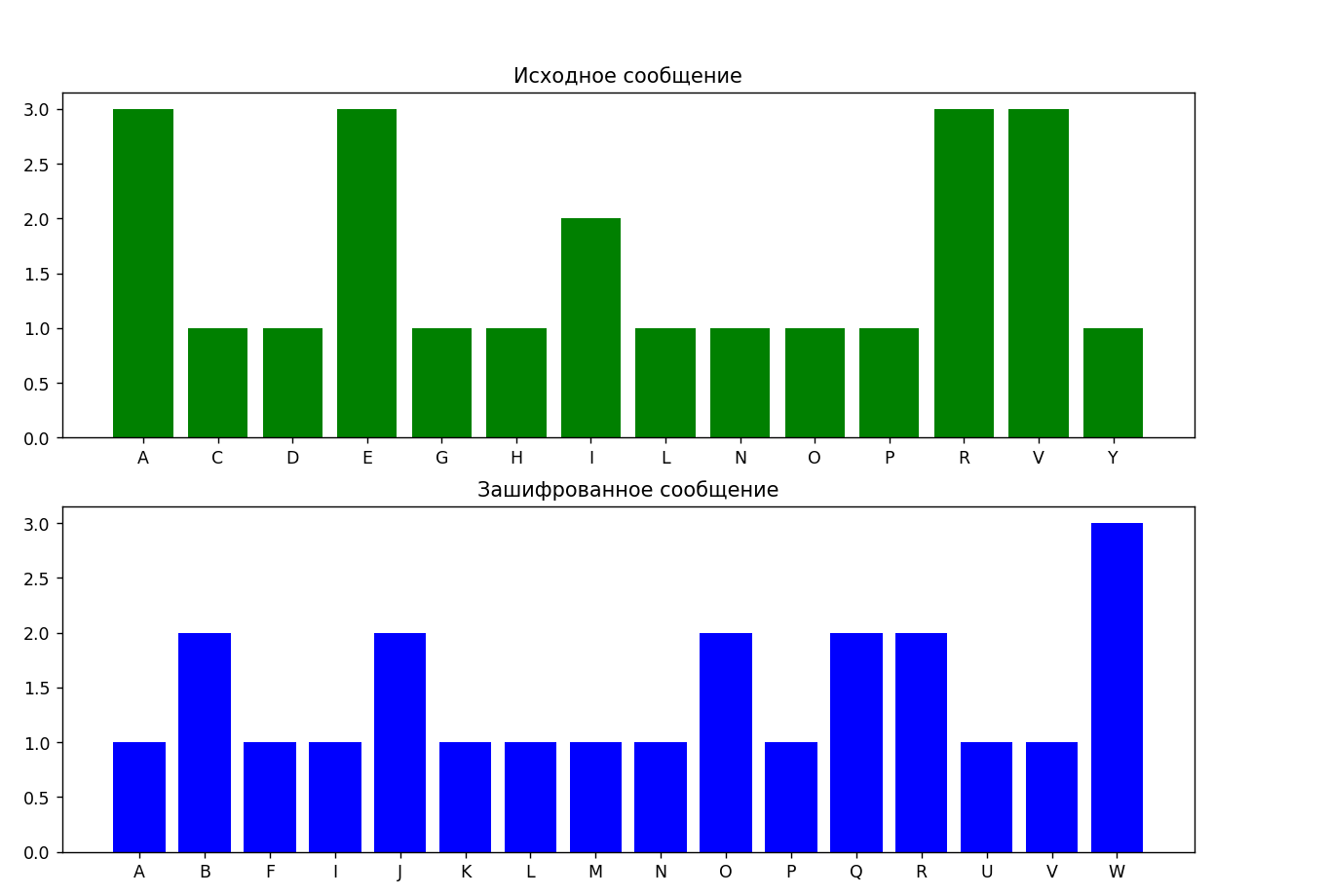


Рисунок 5 – Диаграмма частот сообщения собственного ФИО

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.