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 №4 НА ТЕМУ:

Изучение устройства и функциональных особенностей шифровальной машины «Энигма»

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 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.

**Теоретические сведения**

Машина «Энигма» – это электромеханическое устройство. Как и другие роторные машины, «Энигма» состоит из комбинации механических и электрических подсистем.

Механическая подсистема состоит из:

- клавиатура;

- роторы;

- ступенчатый механизм.

Электрическая подсистема состоит из:

- электрическая схема (соединяет клавиатуру, коммутационную панель, лампочки и роторы).

На рис. 1 показана фотография одной из моделей «Энигмы» с указанием месторасположения основных модулей машины. Как видно на этом рисунке, «Энигма» состоит из пяти 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, замыкает цепь);

- коммутационной панели *4* (дополнительно меняют местами электрические соединения (контакты) двух букв);

- панели в виде электрических лампочек *5* (демонстрирует выходные буквы в процессе шифрования).

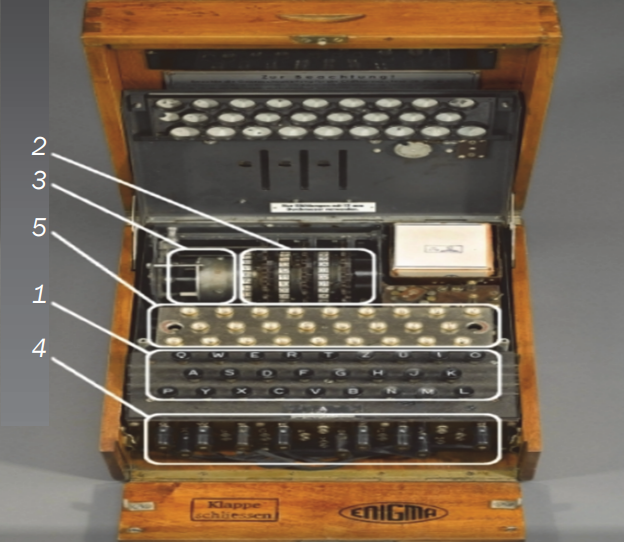


Рисунок 1 – Внешний вид трехроторной "Энигмы"

Общий принцип работы: 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.

Механические части двигались и, замыкая контакты, образовывали меняющийся электрический контур. При нажатии на клавишу клавиатуры контур замыкается, ток проходит через созданную (для зашифрования/расшифрования одного конкретного символа сообщения) цепь и в результате включает одну из набора лампочек, отображающую искомую букву шифртекста (или расшифрованного сообщения).

Принято считать, что в основе шифра «Энигмы» лежит динамический шифр цезаря.

**Ход работы**

Для выполнения лабораторной работы были использованы данные варианта 12.

**Задание 1.**

Ознакомиться с функционалом симулятора «Энигма». Произвести зашифрование сообщения (собственные имя, 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.

Был использован онлайн симулятор «Энигмы»: [*https://piotte13.github.io/enigma-cipher/*](https://piotte13.github.io/enigma-cipher/).

На рисунке 2 представлена первая попытка зашифровать сообщение «*ElizavetaShimchenok*». При этом используется три ротора (I, II, III, начиная с правого), релектор *B*, роторы не смещаются. Внизу изображения продемонстрирована выходная последовательность – шифртекст. Чтобы расшифровать шифртекст, нужно использовать его как входное сообщение – в результате будет введенные фамилия и имя.

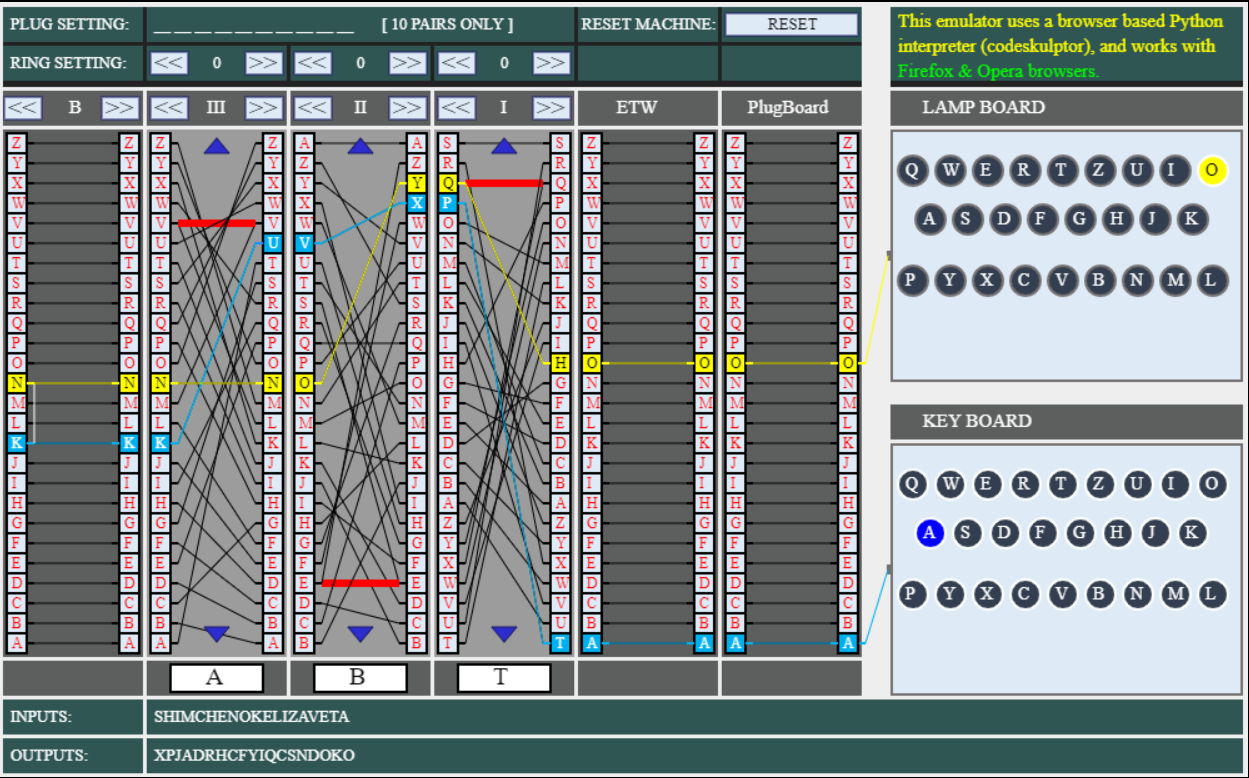


Рисунок 2 – Симулятор "Энигма"

На рисунке 3 изображена еще одна попытка зашифровки, но с роторами (I, II, III), рефлектором *C* и смещением всех роторов на один шаг.

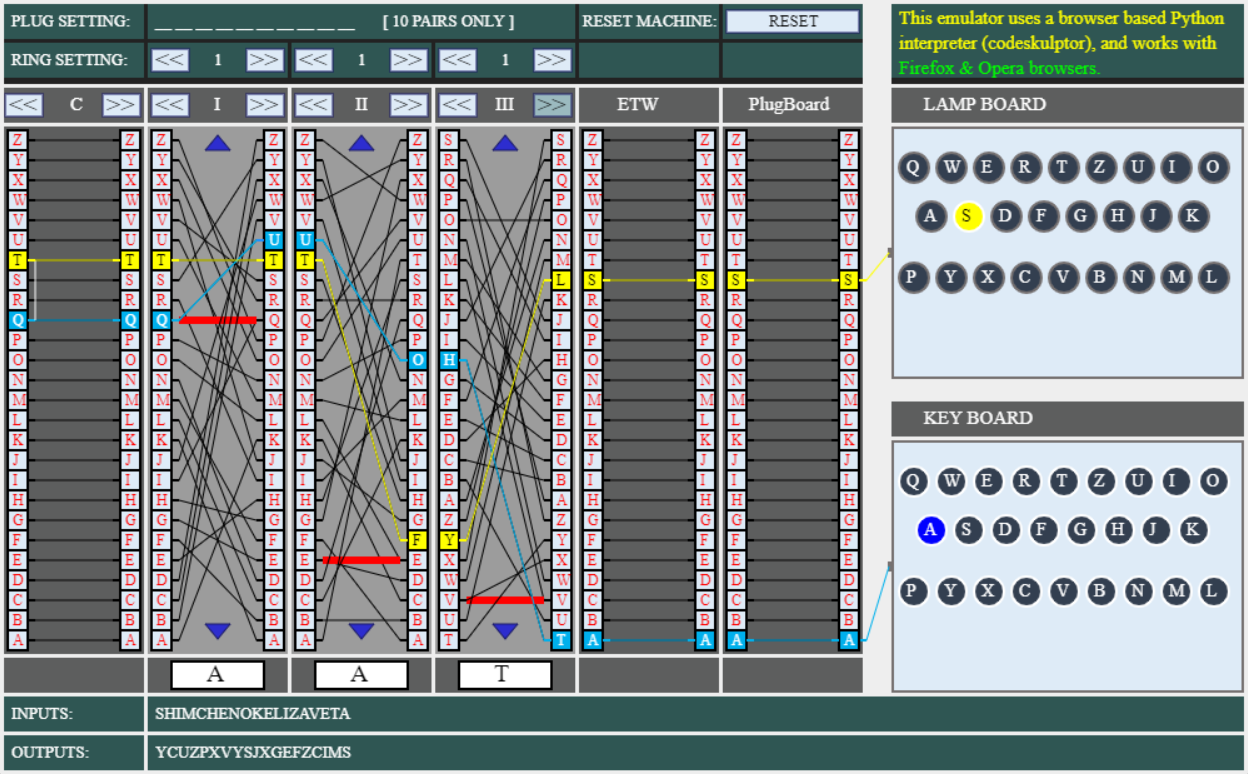


Рисунок 3 – Симулятор "Энигма"

Исходя из диаграмм встречи символов в исходном и зашифрованном сообщениях, изображенных на рисунке 4, можно сказать, что частота появления символов между исходным текстом и шифртекстом никак не связана.

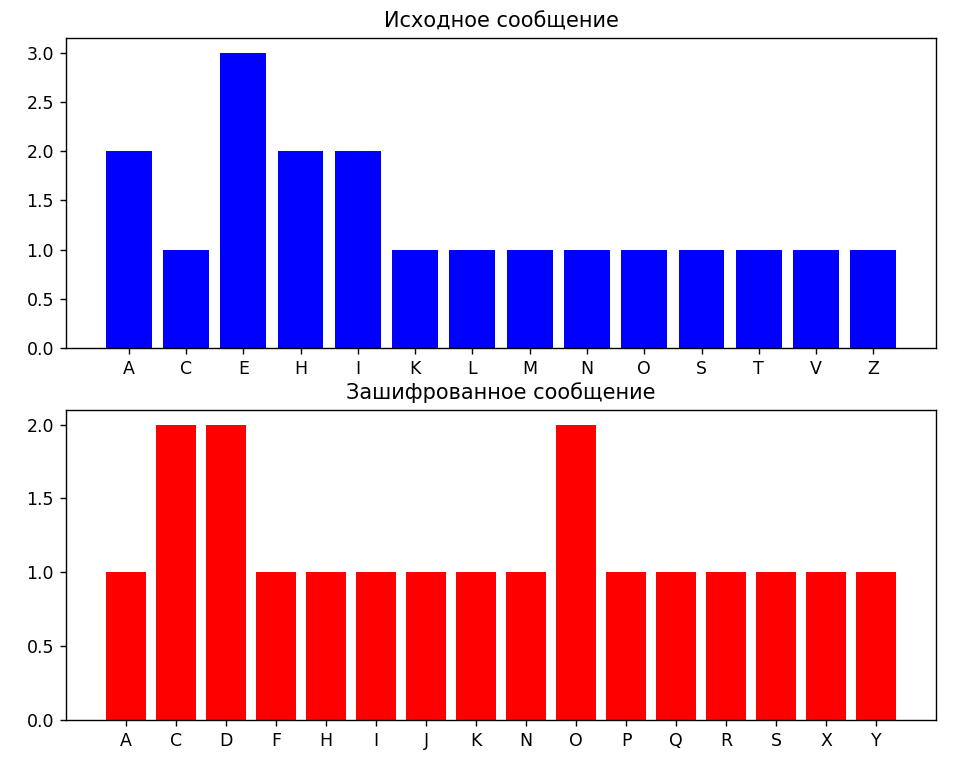
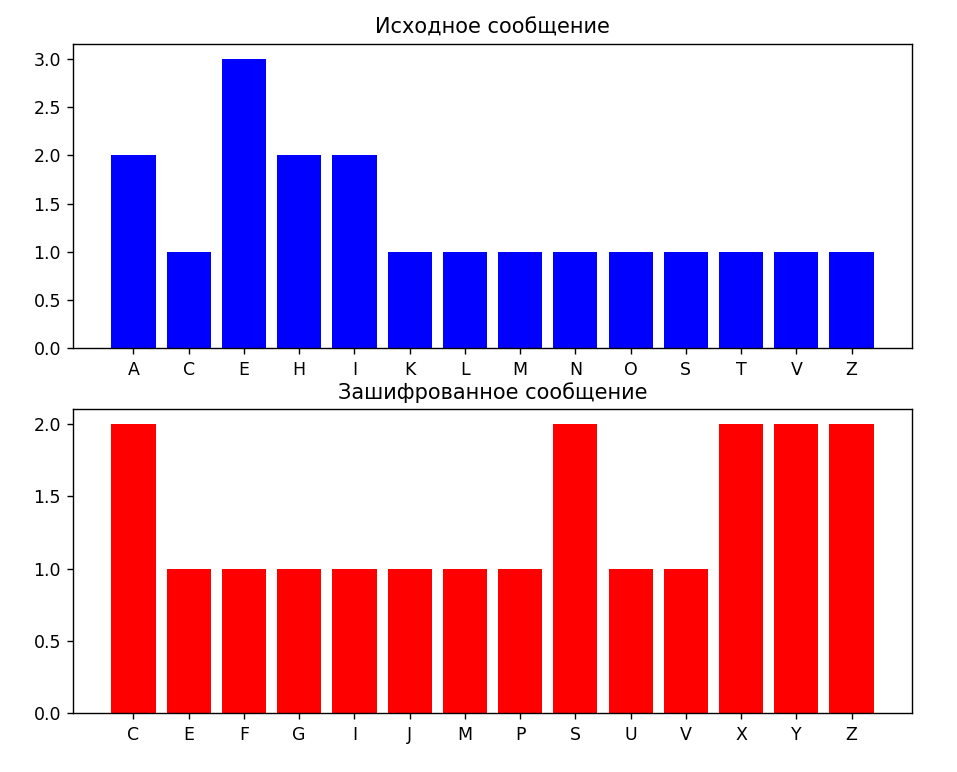
 

Рисунок 4 – Частотные свойства символов исходного текста и двух шифртекстов

**Задание 2.**

Разработать приложение-симулятор шифровальной машины, состоящей из трех роторов и отражателя.

Таблица 1 – Исходные данные

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *L* | *M* | *R* | *Re* | *Li-Mi-Ri* |
| III | *Gamma* | V | *C Dunn* | 1-1-2 |

Рассмотрим процесс зашифрования поэтапно на примере одного символа «*E*» без смещения роторов. Предположим также, что они находятся в своем положении *A*, когда выполняется шифрование.

Сначала правый *R* ротор делает подстановку в соответствии со своим алфавитом. Буква «*E*» заменится на «*G*».

**ABCD E FGHIJKLMNOPQRSTUVWXYZ**

**VZBR G ITYUPSDNHLXAWMJQOFECK**

Далее средний *M* ротор заменит букву «*G*» на «*U*».

**ABCDEF G HIJKLMNOPQRSTUVWXYZ**

**FSOKAN U ERHMBTIYCWLQPZXVGJD**

Далее левый *L* ротор заменит букву «*U*» на «*K*».

**ABCDEFGHIJKLMNOPQRST U VWXYZ**

**BDFHJLCPRTXVZNYEIWGA K MUSQO**

Далее используется рефлектор *C Dunn*, который также в свою очередь подставляет буквы, но подстановок у него всего тринадцать. Здесь буква «*K*» заменится на «*H*».

**ABCDEFGHIJ K LMNOPQRSTUVWXYZ**

**RDOBJNTKVE H MLFCWZAXGYIPSUQ**

Теперь замена будет в обратную сторону: к левому ротору, центральному и правому. Замена будет следующей: *H* – *P* – *C* – *B*.

В результате буква «*E*» будет зашифрована в букву «*B*». На рисунке 5 продемонстрирована проверка с помощью разработанного приложения.

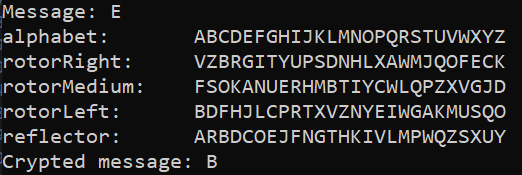


Рисунок 5 – Зашифровка символа «E» без смещений роторов

Учитывая все данные из таблицы 1, я реализовала зашифровку сообщения, состоящего из своего ФИО (Рис. 6). Использовалось три ротора, их начальные позиции не изменялись, и рефлектор *C Dunn*. В приложении при каждом клике на клавишу правый ротор проворачивается на два символа, затем происходит зашифровка символа исходного сообщения. Когда правый ротор проворачивается один цикл – 26 раз, – центральный ротор проворачивается на один символ. Когда центральный проходит цикл – левый ротор тоже проворачивается на один символ.

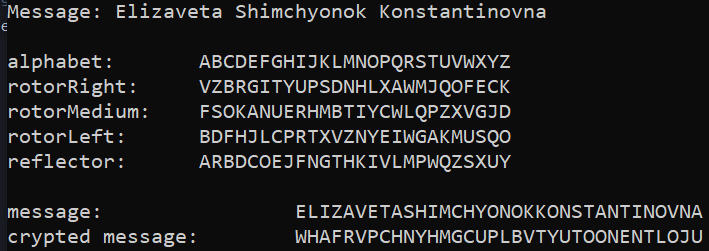


Рисунок 6 – Зашифровка ФИО в соответствии с вариантом

Теперь зашифруем сообщение при помощи пяти разных настроек установок роторов (Рис. 7).

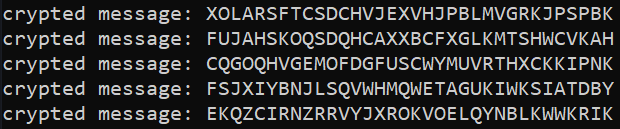


Рисунок 7 – Зашифровка ФИО в соответствии с вариантом

Моя модель Энигмы имеет 3 различных ротора. 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 букв 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.

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.

**Ответы на 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.**

По выводам, сделанным в процессе лабораторной работы, можно сказать, что криптостойкость разработанного симулятора такая же, как и у оригинальной машины.

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.

**Вывод:** в ходе лабораторной работы были приобретены навыки разработки и использования шифровальной машины «Энигма». Были изучены основные принципы работы «Энигмы». Также было разработано приложение на языке программирования C# для реализации задач, связанных с шифрованием данных.