**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра ИБ**

**отчет**

**по лабораторной работе №1**

**по дисциплине «Криптографические методы защиты информации»**

**Тема: Изучение классических шифров средствами RailFence, Scytale, Caesar.**

|  |  |  |
| --- | --- | --- |
| Студентка гр. 4383 |  | Гордеева Т.В. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2017

**Цель работы:** исследовать шифры Rail Fence, Scytale, Caesar и получить практические навыки работы с ними, в том числе и в программном продукте Cryptool 1 и 2.

**1 Шифр изгороди (Rail Fence)**

**1.1 Задание**

1. Найти шифр в CrypTool 1: Encrypt/Decrypt-> Symmetric(Classis).

2. Создать файл с открытым текстом, содержащим последовательность цифр.

3. Запустить шифр и выполнить зашифровку и расшифровку созданного текста несколько раз.

4. Установить, как влияют на шифрование параметры Number of Rows и Offset.

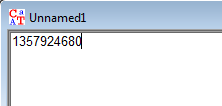
5. Зашифровать и расшифровать текст, содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра при Number of Rows>2, Offset≥2. Убедиться в совпадении результатов.

6. Создайте шифровку для варианта Offset=0 и Number of Rows≤ и передайте коллеге слева для расшифровки.

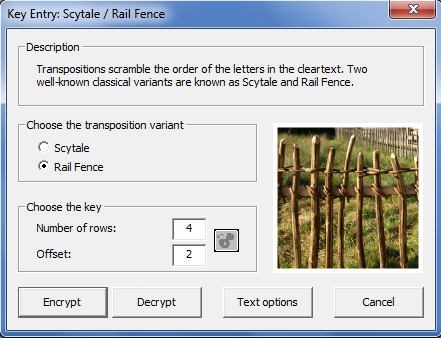
7. Определите ключ методом «грубой силы» и расшифруйте полученный от коллеги шифротекст.

**1.2 Реализация в CrypTool 1.0**

Открытый текст:

Рис.1

Спецификация параметров:

 Рис.2

Number of rows – количество строк

Offset – смещение.

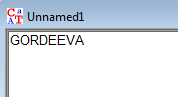
Выполним зашифровку и расшифровку созданного текста несколько раз.

|  |  |  |  |
| --- | --- | --- | --- |
| **Открытый текст** | **Number of rows** | **Offset** | **Результат шифрования** |
| 1357924680 | 4 | 2 | 9720154836 |
| 1357924680 | 4 | 0 | 1432659870 |
| 1357924680 | 2 | 1 | 3726015948 |
| 1357924680 | 2 | 2 | 1594837260 |

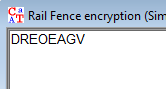
*Таблица 1. Пример работы шифра при заданных параметрах.*

Зашифровать и расшифровать текст, содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра при Number of Rows=4, Offset=3.

Открытый текст:

 Рис.3

Шифротекст:

 Рис.4

# Результат шифрования вручную:

# **. . . . . . D . . . .**

# **. . . . . R . E . . .**

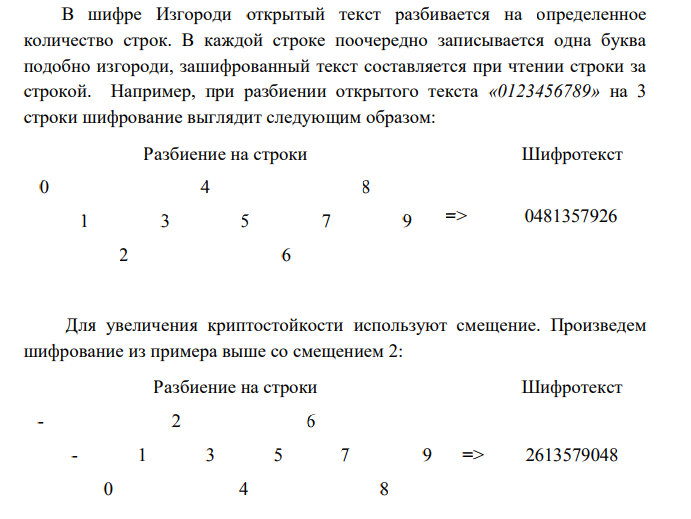
# **. . . . O . . . E . A**

# **. . . G . . . . . V .**

Шифротекст: DREOEAGV

Результаты шифрования вручную и с помощью средства CrypTool 1 совпали.

**1.3 Схема, поясняющая работу шифра**

****

**1.4 Тип шифра**

Тип шифра – перестановка.

**1.5 Ключ шифра**

Ключ шифра – высота забора и смещение..

**1.6 Оценка сложности атаки “грубой силы”**

При длине текста n ключ можно подобрать за n^2 шагов.

**1.7 Результат расшифровки перехваченного от коллеги текста**

Полученный текст: «Itsnia a rsanve, uiiviqtn naao s»

Попробуем определить ключ методом «грубой силы» и расшифруем полученный шифротекст (известно, что парметр offset=0).

*Number of Rows = 7* результат будет – « In vino veritas, in aqua sanitas».

**2 Шифр «Сцитала» (Scytale)**

**2.1 Задание**

1. Найти шифр в CrypTool 1: Encrypt/Decrypt-> Symmetric(Classic).

2. Создать файл с открытым текстом, содержащим последовательность цифр.

3. Запустить шифр и выполнить зашифровку и расшифровку созданного текста несколько раз.

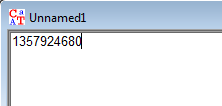
4. Установить, как влияют на шифрование параметры Number of Edges и Offset.

5. Зашифровать и расшифровать текст содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра при Number of Edges > 2, Offset ≥ 2. Убедиться в совпадении результатов.

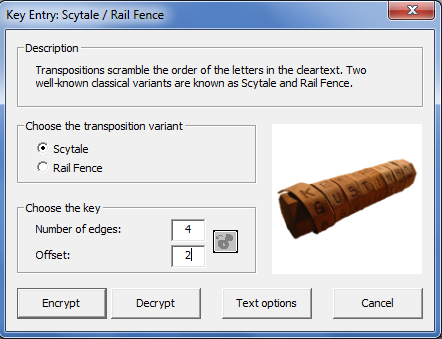
6. Взять в CrypTool 2 шаблон атаки на шифр методом «грубой силы» и модифицировать этот шаблон, заменив блок с шифротекстом на блок ввода открытого текста и блок зашифрования. Изучить принципы этой автоматической атаки.

**2.2 Реализация в CrypTool 1.0**

Открытый текст:

Рис.5

Спецификация параметров:

 Рис.6

Number of rows – количество строк

Offset – смещение.

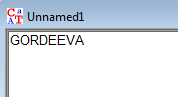
Выполним зашифровку и расшифровку созданного текста несколько раз.

|  |  |  |  |
| --- | --- | --- | --- |
| **Открытый текст** | **Number of rows** | **Offset** | **Результат шифрования** |
| 1357924680 | 4 | 2 | 328540196 |
| 1357924680 | 4 | 0 | 196328540 |
| 1357924680 | 2 | 1 | 214365890 |
| 1357924680 | 2 | 2 | 241638509 |

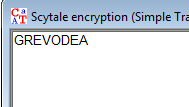
*Таблица 2. Пример работы шифра при заданных параметрах.*

Зашифровать и расшифровать текст, содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра при Number of Rows=5, Offset=2.

Открытый текст:

 Рис.7

Шифротекст:

 Рис.8

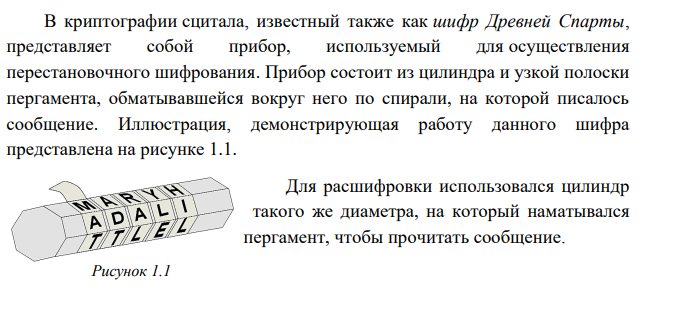
# Результат шифрования вручную:

|  |  |
| --- | --- |
|  |  |
| G | O |
| R | D |
| E | E |
| V | A |

Шифротекст: GREVODEA

Результаты шифрования вручную и с помощью средства CrypTool 1 совпали.

**2.3 Схема, поясняющая работу шифра**

****

**2.4 Тип шифра**

Тип шифра – перестановка.

**2.5 Ключ шифра**

Ключ шифра – количество граней и смещение.

**2.6 Оценка сложности атаки “грубой силы”**

При количестве граней n текст может быть расшифрован не более, чем за n^2 шагов.

**2.7 Описание и оценка сложности атаки “грубой силы” на шифротекст, реализованной в CrypTool 2.**

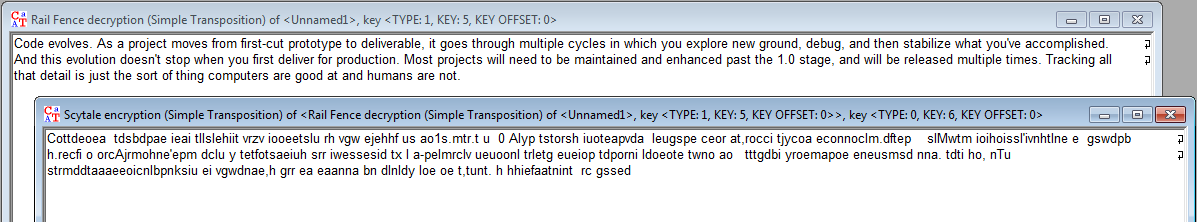


Рис.9 Шифрование заданного текста

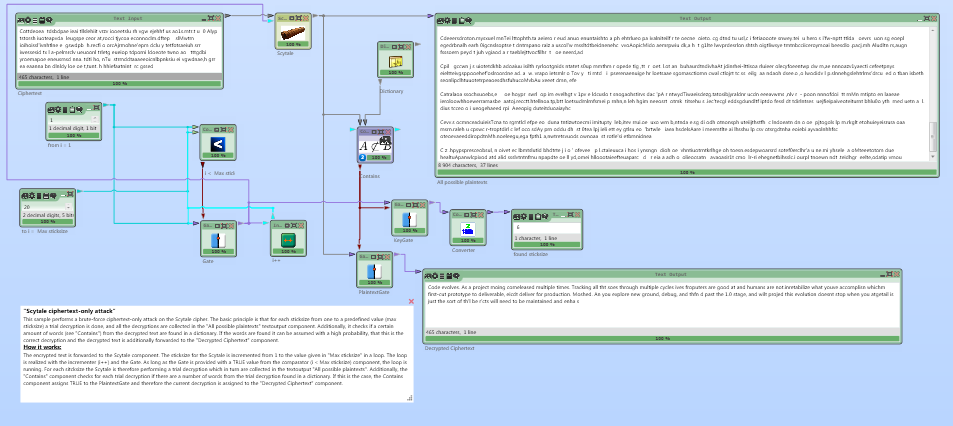


Рис.10

В итоге расшифровки был получен текст.

**3 Шифр Цезаря (Caesar)**

**3.1 Задание**

1. Найти шифр в CrypTool 1: Encrypt/Decrypt->Symmetric(Classic).

2. Зашифровать и расшифровать текст, содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра с ключом, отличным от 0. Убедиться в совпадении результатов.

3. Построить гистограмму частот букв английского языка по эталонному файлу English.txt (папка CrypTool/reference), используя утилиту

из Analysis-> Tools foAnalysis.

4. Зашифровать ключом отличным от 0 файл CrypTool-en.txt (папка CrypTool/Examples).

5. Построить гистограмму частот букв в зашифрованном тексте,

сравнить визуально гистограммы и подтвердить ключ зашифрования.

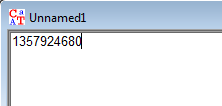
6. Проверить гипотезу о значении ключа утилитой Analysis->

Symmetric Encryption(Classic)->Cipher Text Only->Caesar.

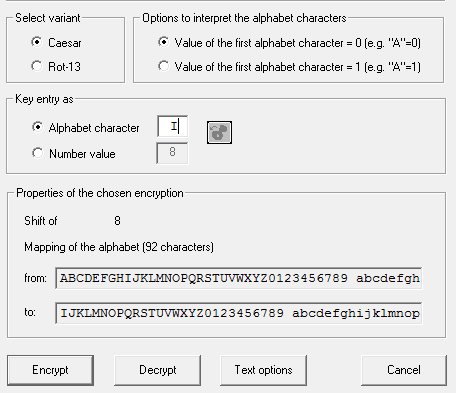
7. Передать шифровку соседу слева для проведения подобной атаки.

**3.2 Реализация в CrypTool 1.0**

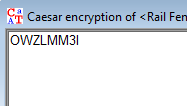
Открытый текст:

Рис.11

Спецификация параметров:

 Рис.12

Шифротекст:

 Рис.13

Результаты шифрования вручную и с помощью средства CrypTool 1 совпали.

Построим гистограмму частот букв английского языка по эталонному файлу English.txt

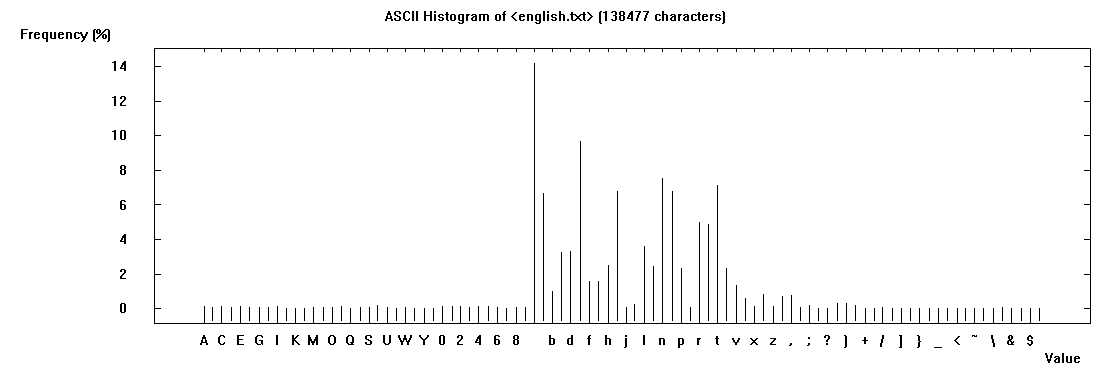
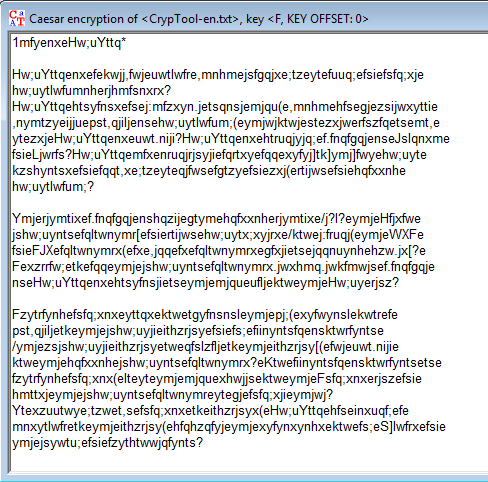


Рис.14

Зашифруем ключом 5 файл CrypTool-en.txt (папка CrypTool/Examples).

 Рис.15

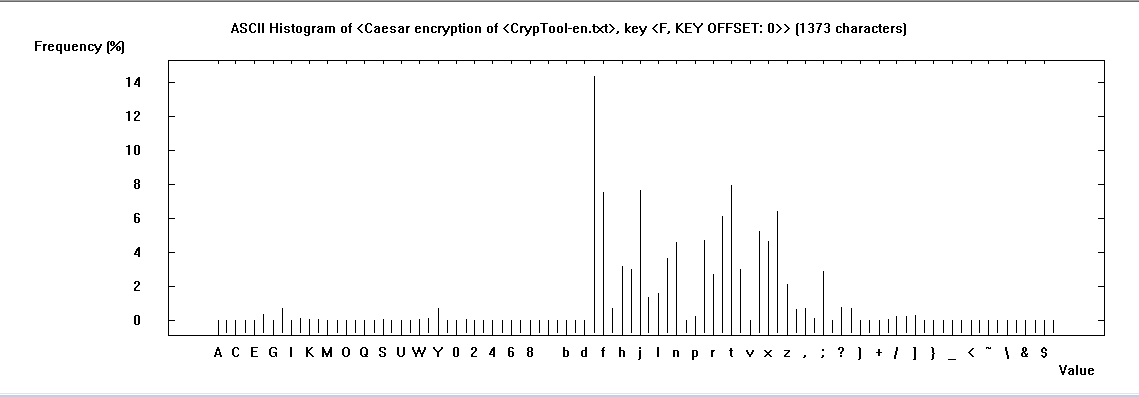
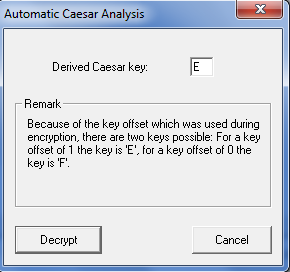
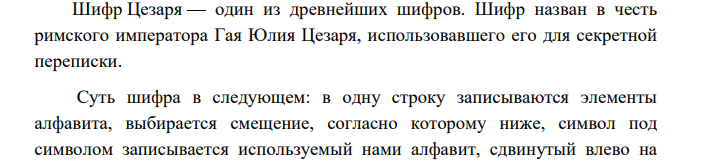


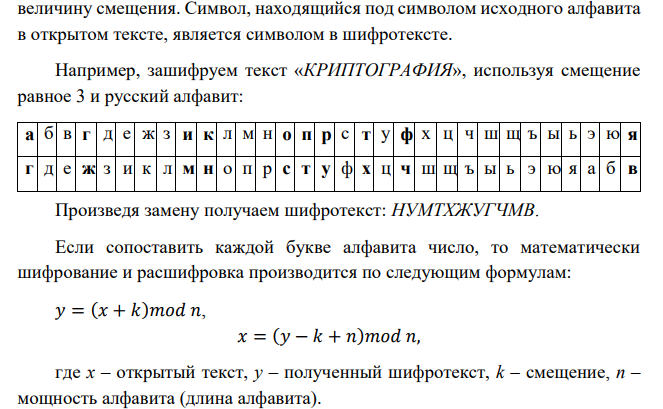
Рис.16 Гистограмма частот букв в зашифрованном тексте

Проверим гипотезу о значении ключа Analysis->Symmetric Encryption(Classic)->Cipher Text Only->Caesar

 Рис.17

**3.3 Схема, поясняющая работу шифра**

****

****

**3.4 Тип шифра**

Тип шифра – замена.

**3.5 Ключ шифра**

Ключ шифра – смещение по алфавиту.

**3.6 Оценка сложности атаки “грубой силы”**

В алфавите длины n текст может быть расшифрован не более чем за n-1 шагов.

**4 Вывод**

В ходе выполнения данной лабораторной работы были изучены с помощью средств CrypTool 1 и CrypTool 2 классические шифры: Шифр “Изгороди”, Шифр “Сцитала”, Шифр “Цезаря”.

Результатом данной лабораторной работы стало изучение алгоритмов шифровки и дешифровки сообщений, также произведена оценка сложности атаки “грубой силой” для каждого шифра.

Для каждого шифра получили следующие выводы:

* Шифр “Изгороди”

Тип шифра – перестановка.

Ключ шифра – высота забора и смещение.

При длине текста n ключ можно подобрать за n^2 шагов.

* Шифр “Сцитала”

Тип шифра – перестановка.

Ключ шифра – количество граней и смещение.

Количестве граней n ключ можно подобрать за n^2 шагов.

* Шифр “Цезаря”

Тип шифра – замена.

Ключ шифра – смещение по алфавиту.

В алфавите длины n текcт может быть расшифрован не более чем за n-1 шагов.

**5 Список источников**

* А. К. Племянников, Е.О. Кузнецова Криптографические методы защиты информации: лабораторный практикум. СПбГЭТУ «ЛЭТИ», 2016 55 с.