**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра ИБ**

**отчет**

**по лабораторной работе №2**

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

**Тема: Изучение классических шифров Substitution, Permutation/Transposition, Vigenere**

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

Санкт-Петербург

2017

**Цель работы:** исследовать шифры Substitution, Permutation/Transposition, Vigenere и получить практические навыки работы с ними, в том числе и в программном продукте Cryptool 1 и 2.

**1 Шифр моноалфавитной подстановки(Substitution)**

**1.1 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 c выбранным ключом и смещением Offset≠ 0. Убедиться в совпадении результатов.

3. Выполнить зашифрование и расшифрование с различными паролями и смещениями Offset и разобраться как формируется алфавит шифрограммы.

4. Выбрать абзац (примерно 600 символов) из файла English.txt (папка CrypTool/reference) и зашифровать его.

5. Выполнить атаку на шифротекст, используя приложение из Analysis-> Symmetric Encryption(classic)-> Cipher Text Only.

6. Повторить шифрование и атаку для тестов примерно в 300 и в 150 символов

7.Изучите ручное расшифрование для текстов менее 300 символов.

8. Выбрать новый абзац (примерно 600 символов) из файла English.txt (папка CrypTool/reference) и зашифровать его.

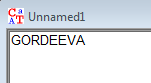
9. Расшифровать этот абзац, используя приложение Analysis-> Tools for Analysis и Analysis-> Symmetric Encryption(classic)-> Manual Analysis.

10. Зашифруйте текст из 200 символов, сохраните ключ, и передайте коллеге для расшифровки.

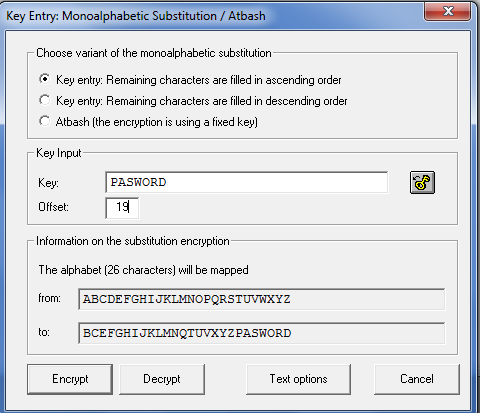
11. Самостоятельно изучите атаки, реализованные CrypTool 2, опираясь на Help и ссылки на статьи.

**1.2 Реализация в CrypTool 1.0**

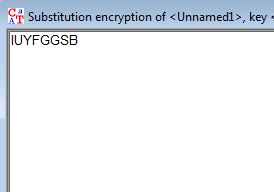
Открытый текст:

Рис.1

Спецификация параметров:

 Рис.2

Шифротекст:

 Рис.3

Результат шифрования вручную:

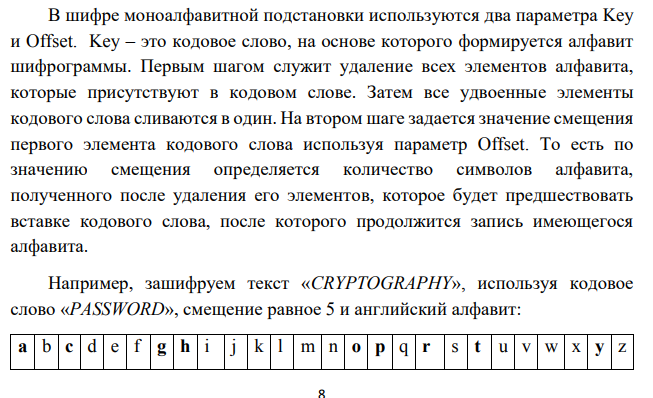
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | B | C | **D** | **E** | F | **G** | H | I | J | K | L | M | N | **O** | P | Q | **R** | S | T | U | **V** | W | X | Y | Z |
| **B** | C | E | **F** | **G** | H | **I** | J | K | L | M | N | Q | T | **U** | P | A | **S** | W | O | R | **D** | V | X | Y | Z |

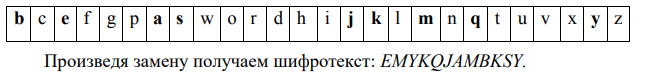
Выполним зашифрование и расшифрование с различными паролями и смещениями Offset.

|  |  |  |  |
| --- | --- | --- | --- |
| **Открытый текст** | **Key** | **Offset** | **Результат шифрования** |
| GORDEEVA | CRYPT | 12 | HYNEFFUA |
| GORDEEVA | CRYPT | 0 | BKNPTTUC |
| GORDEEVA | ELTCH | 5 | LNQFGGVA |
| GORDEEVA | ELTCH | 10 | JHQFGGVA |

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

**1.3 Схема, поясняющая работу шифра**





**1.4 Тип шифра**

Тип шифра – замена.

**1.5 Ключ шифра**

Ключ шифра – ключевое слово без повторяющихся символов и смещение по алфавиту.

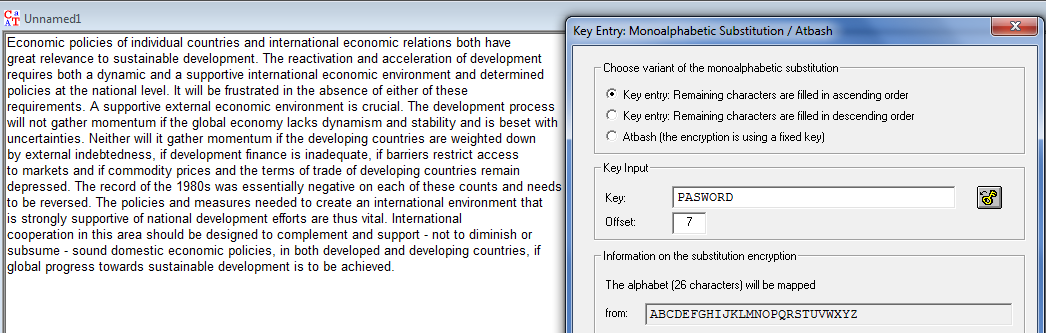
**1.6 Оценка сложности атаки “грубой силы”**

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

**1.7 Описание атаки на шифр с использованием утилит CrypTool 1.0.**

Зашифруем абзац (примерно 600 символов) из файла English.txt

(папка CrypTool/reference).

 Рис.4

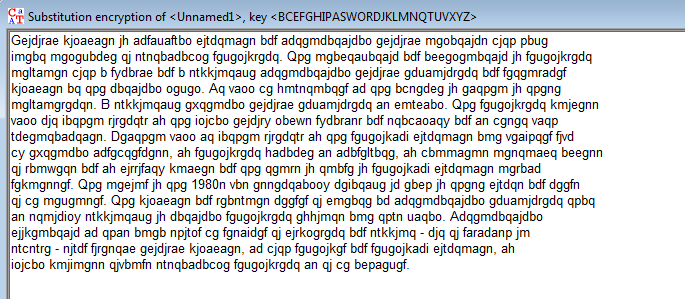


Рис.5

Выполним атаку на шифротекст, используя приложение из Analysis-> Symmetric Encryption(classic)-> Cipher Text Only.

 Рис.6

Повторим шифрование и атаку для тестов примерно в 300 и в 150 символов.

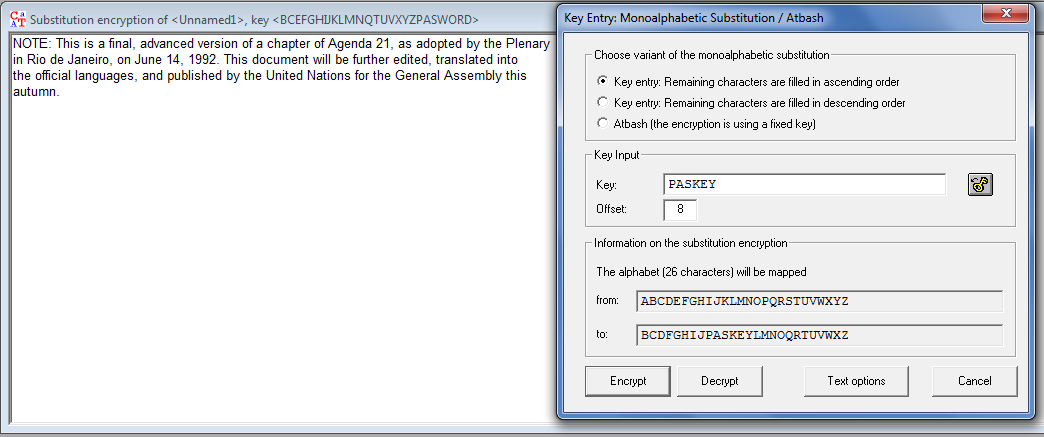


Рис.7 Текст в 300 символов

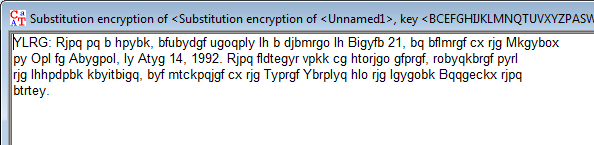


Рис.8

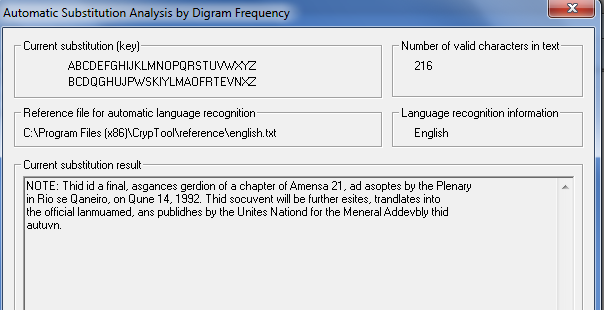


Рис.9

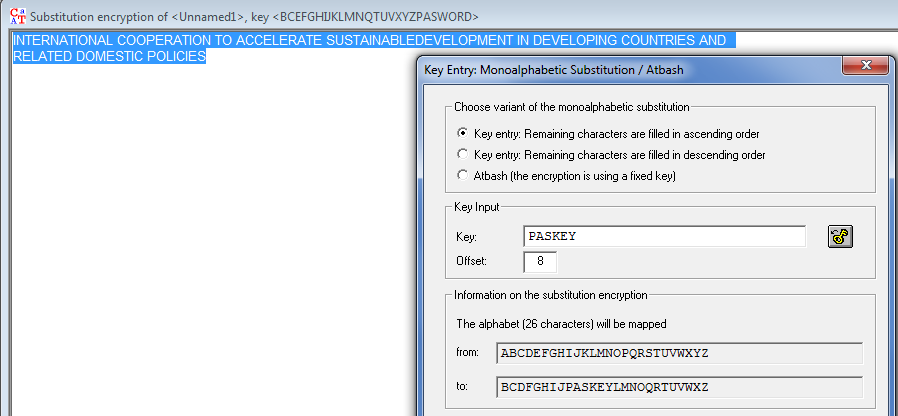


Рис.10 Текст в 150 символов

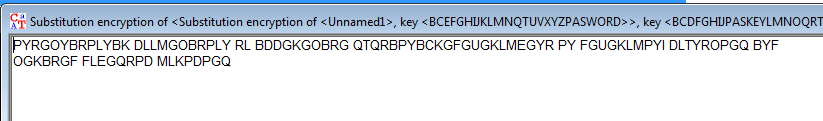


Рис.11

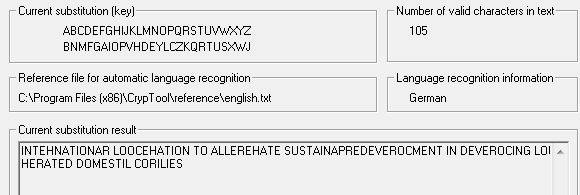


Рис.12

**1.8 Результат расшифровки перехваченного от коллеги текста.**

****

Рис.13 Шифротекст

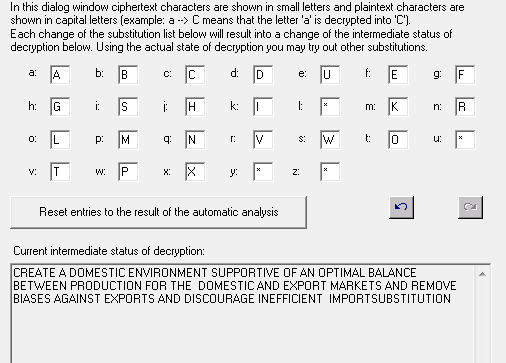


Рис.14 Полученный текст

**1.9 Описание атаки на шифр реализованной в CrypTool 2.0**

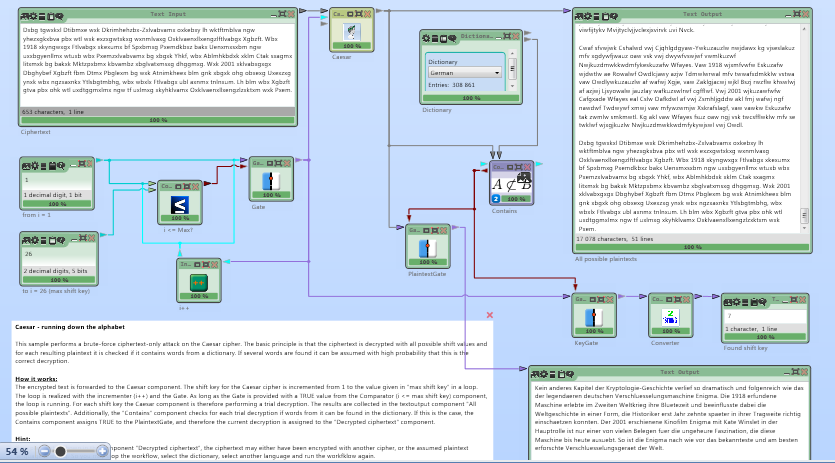
****

Рис.15

**2 Шифр двойной перестановки(Permutation/Transposition)**

**2.1 Задание**

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

2.Зашифровать и расшифровать текст, содержащий ФамилиюИмяОтчество (транслитерация латиницей) вручную и с помощью шифра c ключами для перестановки столбцов и строк. Убедиться в совпадении результатов.

3. Выполнить зашифрование и расшифрование с различными ключами и с различными вариантами перестановки матрицы с текстом по строкам и столбцам. Разобраться с параметрами утилиты.

4. Зашифровать текст, содержащий ФамилиюИмяОтчество и провести атаку, основанную на знании исходного текста Analysis-> Symmetric Encryption(classic)-> Known Plaintext.

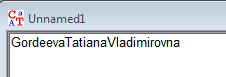
5. Зашифровать текст с произвольным сообщением в формате «DEAR messagе THANKS», используя только одинарную перестановку.

6. Передайте шифровку соседу, для расшифрования при условии, что формы обращения и завершения письма известны.

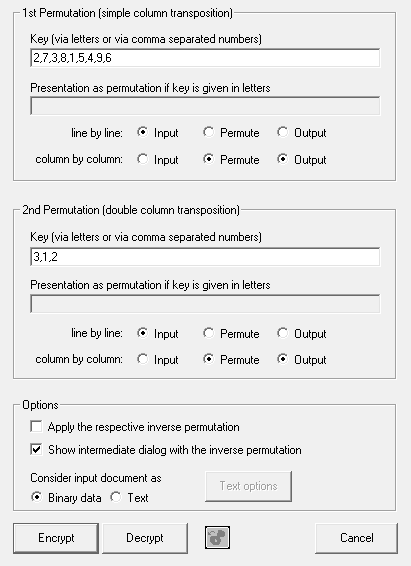
7. Самостоятельно изучите атаки, реализованные в CrypTool 2, опираясь на Help и ссылки на статьи.

**2.2 Реализация в CrypTool 1.0**

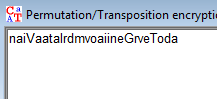
Открытый текст:

Рис.16

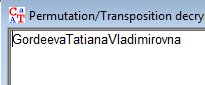
Спецификация параметров:

Рис.17

Шифротекст:

 Рис.18

Расшифрованный текст:

 Рис.19

# Результат шифрования вручную:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **2** | **7** | **3** | **8** | **1** | **5** | **4** | **9** | **6** |
| **3** | G | O | R | D | E | E | V | A | T |
| **1** | A | T | I | A | N | A | V | L | A |
| **2** | D | I | M | I | R | O | V | N | A |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
| **3** | E | G | R | V | E | T | O | D | A |
| **1** | N | A | I | V | A | A | T | A | L |
| **2** | R | D | M | V | O | A | I | I | N |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
| **1** | N | A | I | V | A | A | T | A | L |
| **2** | R | D | M | V | O | A | I | I | N |
| **3** | E | G | R | V | E | T | O | D | A |

Зашифрованный текст: NAIVAATAIRDMVOAIINEGRVETODA

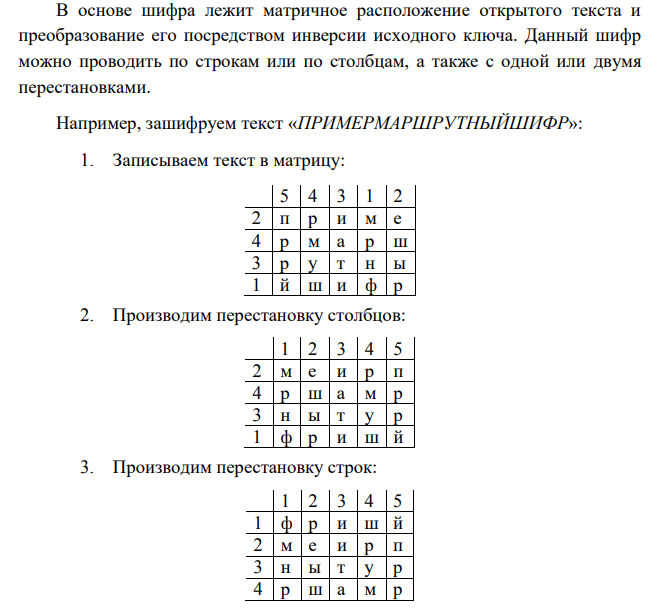
Результаты шифрования вручную и с помощью средства CrypTool 1 совпали.

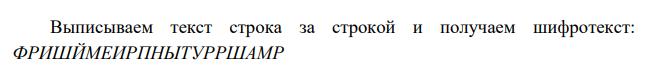
Выполним зашифрование и расшифрование с различными ключами и с различными вариантами перестановки матрицы с текстом по строкам и столбцам.

|  |  |  |  |
| --- | --- | --- | --- |
| **Открытый текст** | **Перестановка по строкам** | **Перестановка по столбцам** | **Результат шифрования** |
| GORDEEVATATIANAVLADIMIROVNA | 4,2,1,3 | 6,4,1,2,7,3,5 | LAIVMINATATNADOVARGERDEOVAI |
| GORDEEVATATIANAVLADIMIROVNA | 2,1,3,8,5,9,4,6,10,7 | 2,1,3 | EVIODTAAAIIANVMRVGETAALDONR |

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

**2.3 Схема, поясняющая работу шифра**

****

****

**2.4 Тип шифра**

Тип шифра – перестановка.

**2.5 Ключ шифра**

Ключ шифра – порядок перестановки по строкам и по столбцам.

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

При количестве строк n и количестве столбцов m сложность атаки “грубой силы” n!\*m!.

**2.7 Результат расшифровки перехваченного от коллеги текста.**

Рис.20 Шифротекст

**2.8 Описание атаки на шифр реализованной в CrypTool 2.0.**

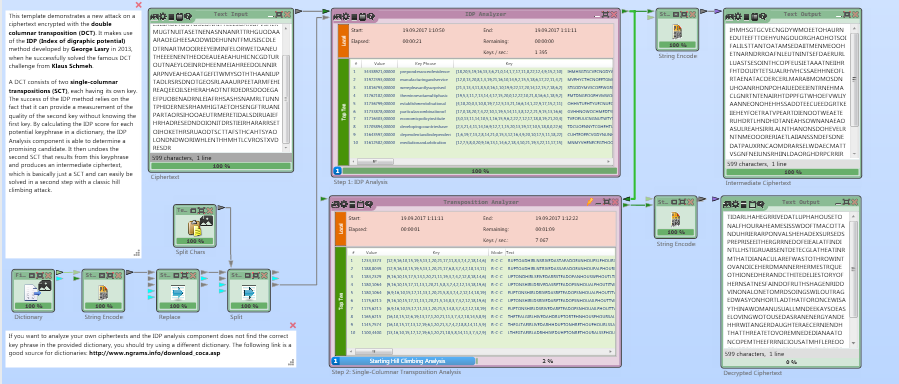


Рис.21

**3 Шифр Виженера (Vigenere)**

**3.1 Задание**

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

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

3. Произвести атаку на шифротекст, используя приложение Analysis-> Symmetric Encryption(Classic)-> Cipher Text Only->Vigenere.

4. Повторить атаку для фрагмента текста из файла English.txt (папка CrypTool/reference). Размер текста не менее 1000 символов.

5. Воспроизведите эту атаку в автоматизированном режиме:

a. Определите размер ключа с помощью приложения Analysis-

> Tools for Analysis-> Autocorrelation

b. Выполните перестановку текста с размером столбца равным

размеру ключа приложением Permutation/Transposition

c. Определите очередную букву ключа приложением Analysis-

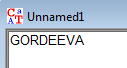
> Symmetric Encryption(Classic)-> Cipher Text Only->Caesar.

6. Самостоятельно изучите атаки, реализованные CrypTool 2,

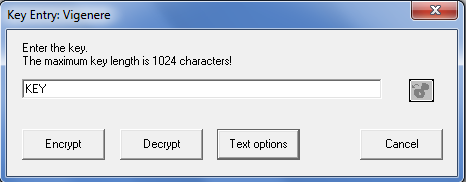
опираясь на Help и ссылки на статьи.

**3.2 Реализация в CrypTool 1.0**

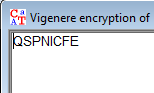
Открытый текст:

Рис.22

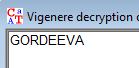
Спецификация параметров:

Рис.23

Шифротекст:

Рис.24

Расшифрованный текст:

Рис.25

Результат шифрования вручную:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **G** | **O** | **R** |  | **D** | **E** | **E** |  | **V** | **A** |  |
| K | E | Y |  | K | E | Y |  | K | E |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | **G** | H | I | J | K | L | M | N | **O** | P | Q | **R** | S | T | U | V | W | X | Y | Z |
| K | L | M | N | O | P | **Q** | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| E | F | G | H | I | J | K | L | M | N | O | P | Q | R | **S** | T | U | V | W | X | Y | Z | A | B | C | D |
| Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | **P** | Q | R | S | T | U | V | W | X |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | **D** | **E** | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| K | L | M | **N** | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| E | F | G | H | **I** | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| Y | Z | A | B | **C** | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | **V** | W | X | Y | Z |
| K | J | K | L | M | N | Q | T | U | P | A | S | W | O | R | D | V | X | Y | Z | C | **E** | F | G | H | I |
| **E** | G | H | I | J | K | L | M | N | Q | T | U | P | A | S | W | O | R | D | V | X | Y | Z | C | E | F |
| Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |

Зашифрованный текст: QSPNICEE

Результаты шифрования вручную и с помощью средства CrypTool 1 совпали.

Произведем атаку на шифротекст, используя приложение Analysis- > Symmetric Encryption(Classic)-> Cipher Text Only->Vigenere.

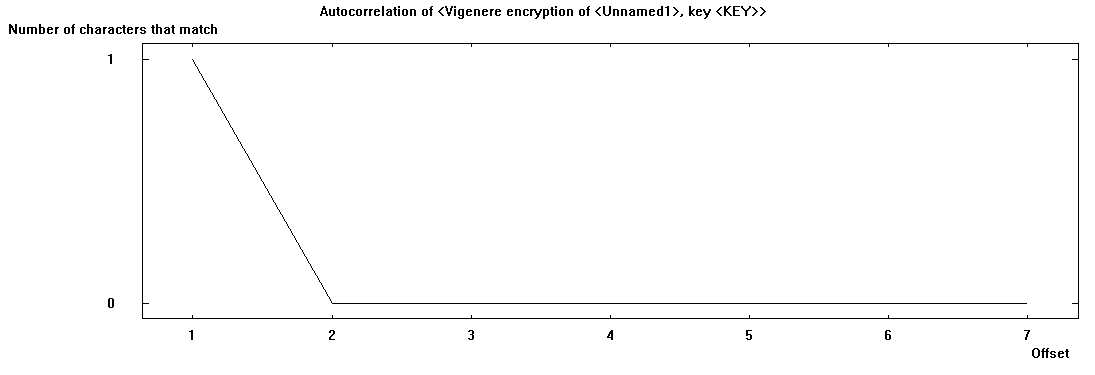
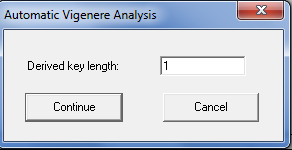
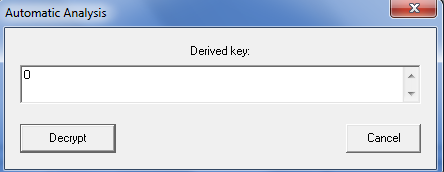
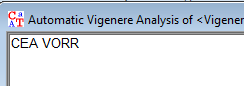
****

Рис.26

**** Рис.27

**** Рис.28

**** Рис.29

При атаке на шифротекст с помощью средств СrypTool 1.0 был получен ключ, не совпадающий с нашим, в итоге получить исходный текст не удалось.

Повторим атаку для фрагмента текста из файла English.txt (папка CrypTool/reference). Размер текста не менее 1000 символов.

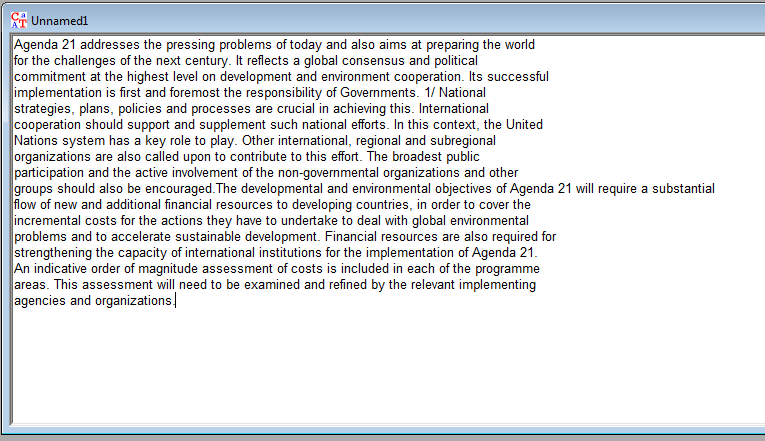


Рис.30

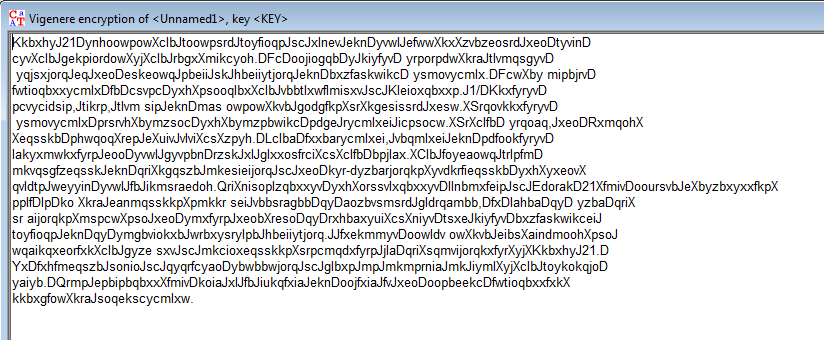


Рис.31

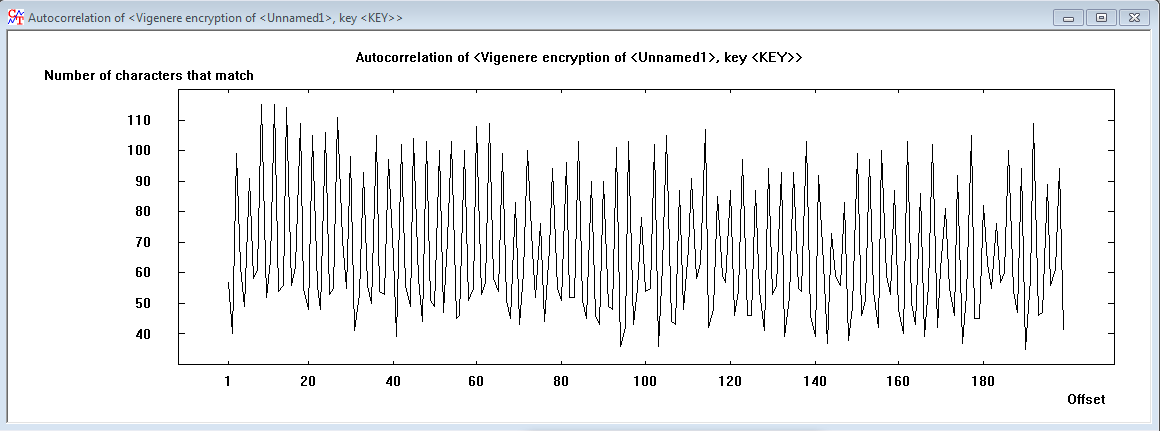
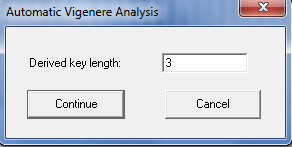
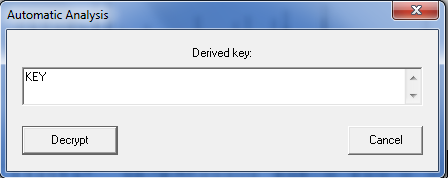


Рис.32

Рис.33

Рис.34

Программа распознала ключ верно.

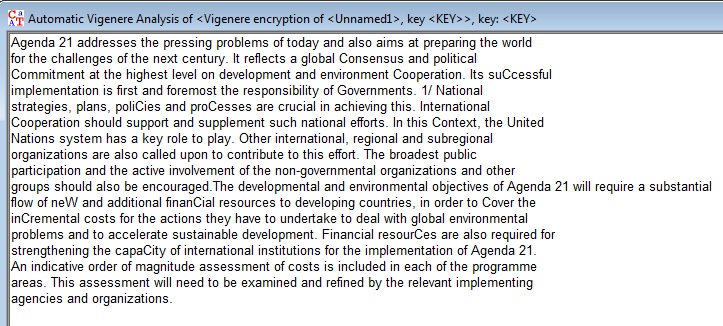


Рис.35

Воспроизведем эту атаку в автоматизированном режиме:

a. Определим размер ключа с помощью приложения Analysis-> Tools for Analysis-> Autocorrelation

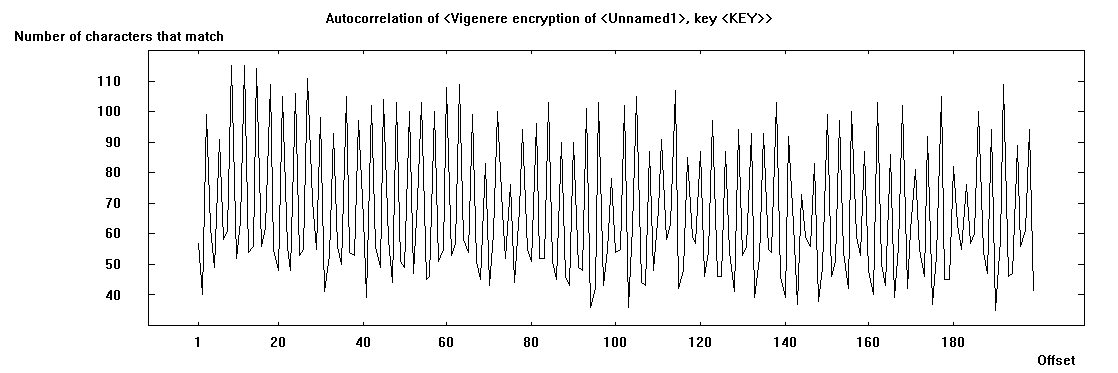
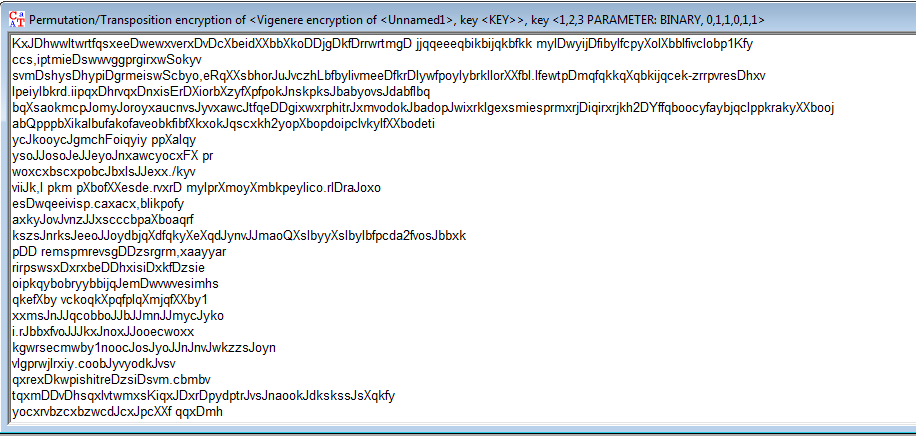
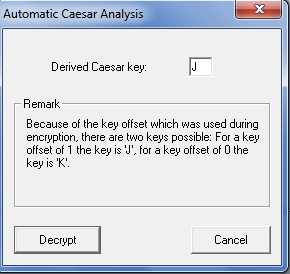


Рис.36

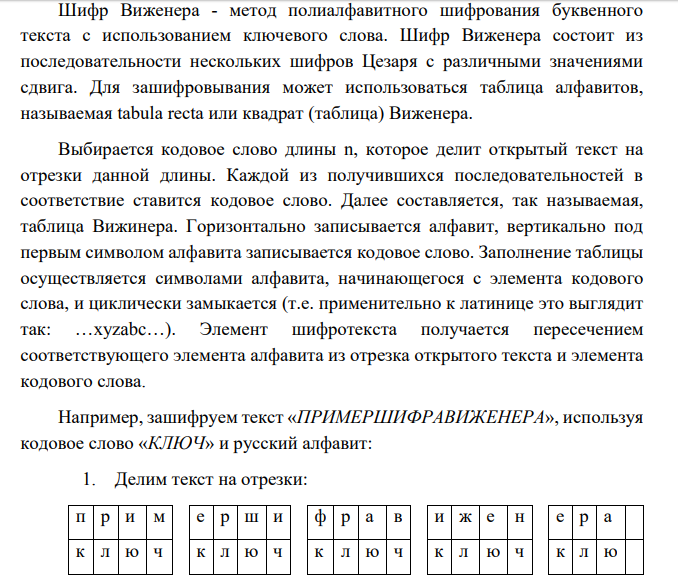
b. Выполним перестановку текста с размером столбца равным размеру ключа приложением Permutation/Transposition

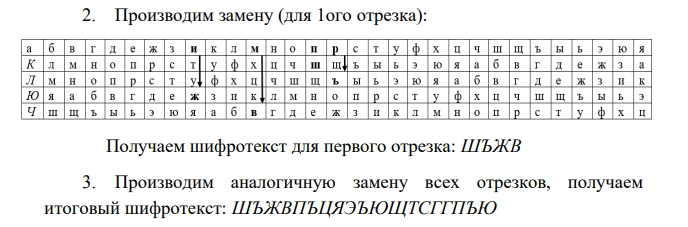
 Рис.37

c. Определим очередную букву ключа приложением Analysis-> Symmetric Encryption(Classic)-> Cipher Text Only->Caesar.

**** Рис.38

**3.3 Схема, поясняющая работу шифра**

****

****

**3.4 Тип шифра**

Тип шифра – замена.

**3.5 Ключ шифра**

Ключ шифра – ключевое слово.

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

При длине алфавита n и длине ключевого слова m сложность атаки “грубой силы” n!\*(n-m)!.

**3.7 Описание атаки на шифр реализованной в CrypTool 2.0**

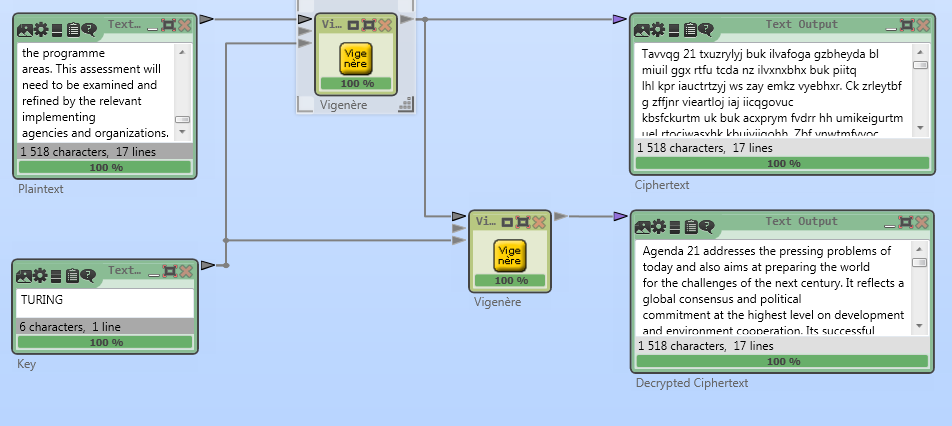


Рис.39

**4 Вывод**

В ходе выполнения данной лабораторной работы были изучены с помощью средств CrypTool 1 и CrypTool 2 классические шифры: Шифр моноалфавитной подстановки, Шифр Двойной Перестановки, Шифр Виженера.

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 моноалфавитной подстановки

Тип шифра – замена.

Ключ шифра – ключевое слово без повторяющихся символов и смещение по алфавиту.

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

Тексты длиной более 600 символов более уязвимы к атаке, а тексты длиной менее 150 символов практически невозможно правильно дешифровать.

* Шифр Двойной Перестановки

Тип шифра – перестановка.

Ключ шифра – порядок перестановки по строкам и столбцам.

При количестве строк n и количестве столбцов m сложность атаки “грубой силы” n!\*m!.

* Шифр Виженера

Тип шифра – замена.

Ключ шифра – ключевое слово.

При длине алфавита n и длине ключевого слова m сложность атаки “грубой силы” n!\*(n-m)!.

**5 Список источников**

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