

**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 Scytale, Vigenere,**  
**Hill»**  
**Вариант 6**

Студент гр. 8383

Киреев К.А.

Преподаватель

Племянников А.К.

Санкт-Петербург

2021

## Цель работы

Исследовать шифры Rail Fence, Vigenere, Hill и получить практические навыки работы с ними, в том числе с использованием приложений Cryptool 1 и 2.

## Шифр “Сцитала”

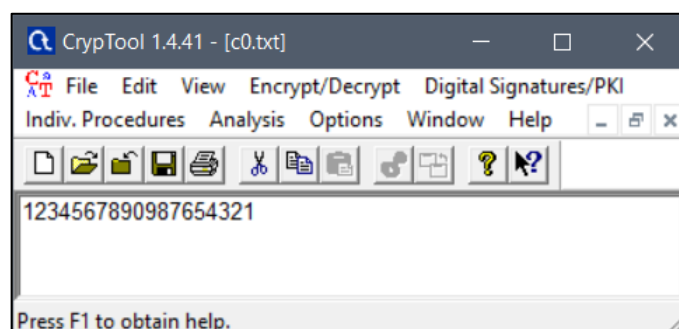
### Задание

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  $\geq$  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.

## Ход работы

### Реализация в CrypTool 1.0

- Создать файл с открытым текстом, содержащим последовательность цифр.



## Рисунок 1 – Открытый текст

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

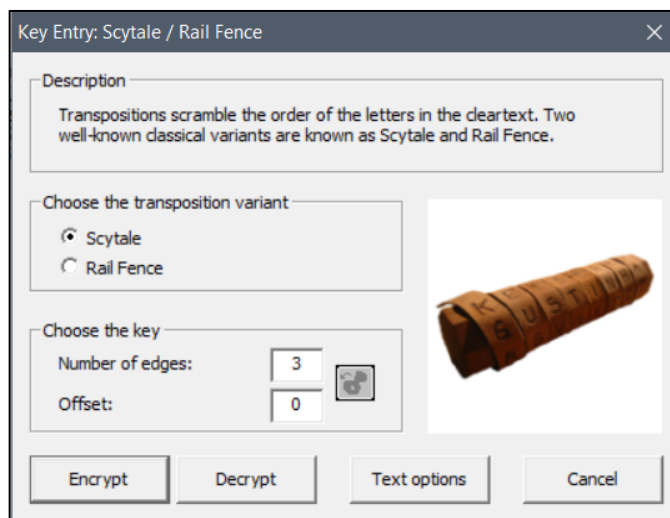


Рисунок 2 – Спецификация параметров

Таблица 1 – Пример работы шифра

Открытый текст	Number of edges (Количество граней)	Offset (Смещение)	Результат шифрования
1234567890987654321	3	0	1852943034925816776
1234567890987654321	4	0	1597326062379514884
1234567890987654321	4	2	5936821771286395404
1234567890987654321	2	5	8909817263544536271
1234567890987654321	2	1	0192837465564738291

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

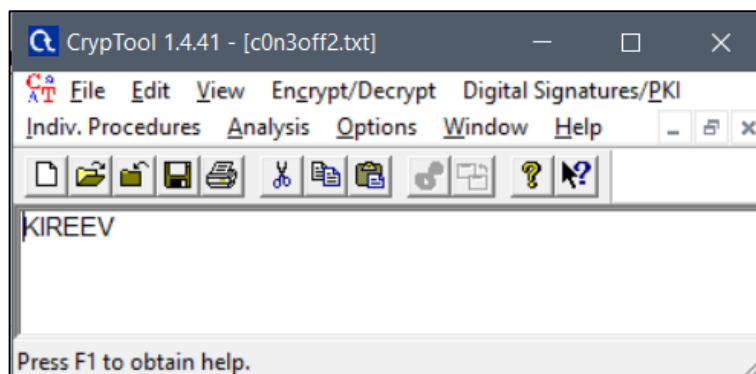


Рисунок 3 – Открытый текст

Параметры шифрования: *Number of Edges* = 3, *Offset* = 2

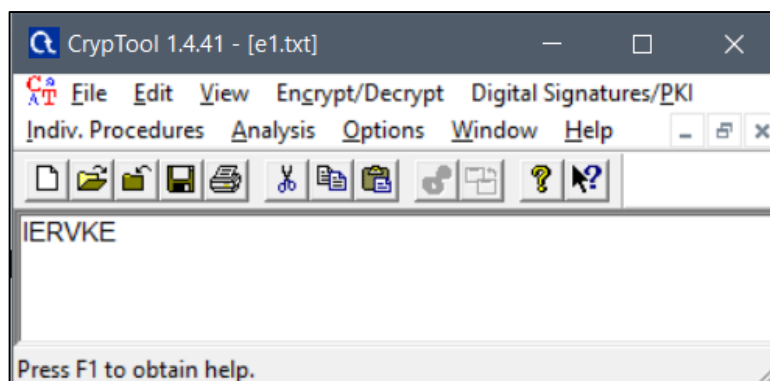


Рисунок 4 – Результат шифрования с помощью программы

Результат шифрования вручную:

-	-	К
I	R	E
E	V	

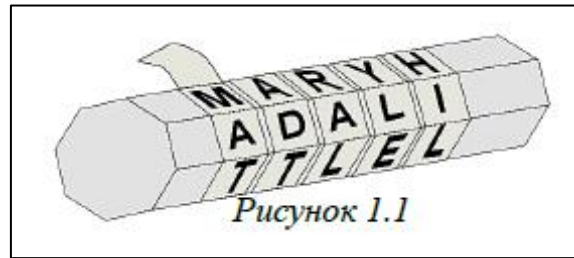
Шифротекст: IERVKE

Результаты шифрования вручную и с помощью CrypTool 1.0 совпали.

### ***Схема, поясняющая работу шифра***

В криптографии шифр «Считала», известный также, как шифр Древней Спарты, представляет собой прибор, используемый для осуществления перестановочного шифрования. Прибор состоит из гранёного цилиндра (жезла) и узкой полоски пергамента, которая обматывается вокруг цилиндра по спирали. На гранях цилиндра записывалось сообщение. Иллюстрация,

демонстрирующая работу данного шифра представлена на рисунке ниже. Для расшифровки использовался гранёный цилиндр такого же диаметра, на который наматывался пергамент, чтобы прочесть сообщение.



### ***Тип шифра***

Тип шифра – перестановка.

### ***Ключ шифра***

Ключ шифра – количество граней и смещение.

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

Атака методом “грубой силы” - полный перебор ключей (секретов) шифра при известном алгоритме зашифровки.

Основной принцип атаки заключается в том, что дешифрование выполняется для всех размеров бара (количество граней) от 1 до заданного значения (максимальный размер бара), а дешифрованные тексты собираются в компоненте со всеми простыми текстами. Кроме того, проверяется, существует ли минимальное количество расшифрованного текста в словаре. Если слова найдены, весьма вероятно, что был найден правильный текстовый текст, а текст также отправлен компоненту «расшифрованный зашифрованный текст».

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

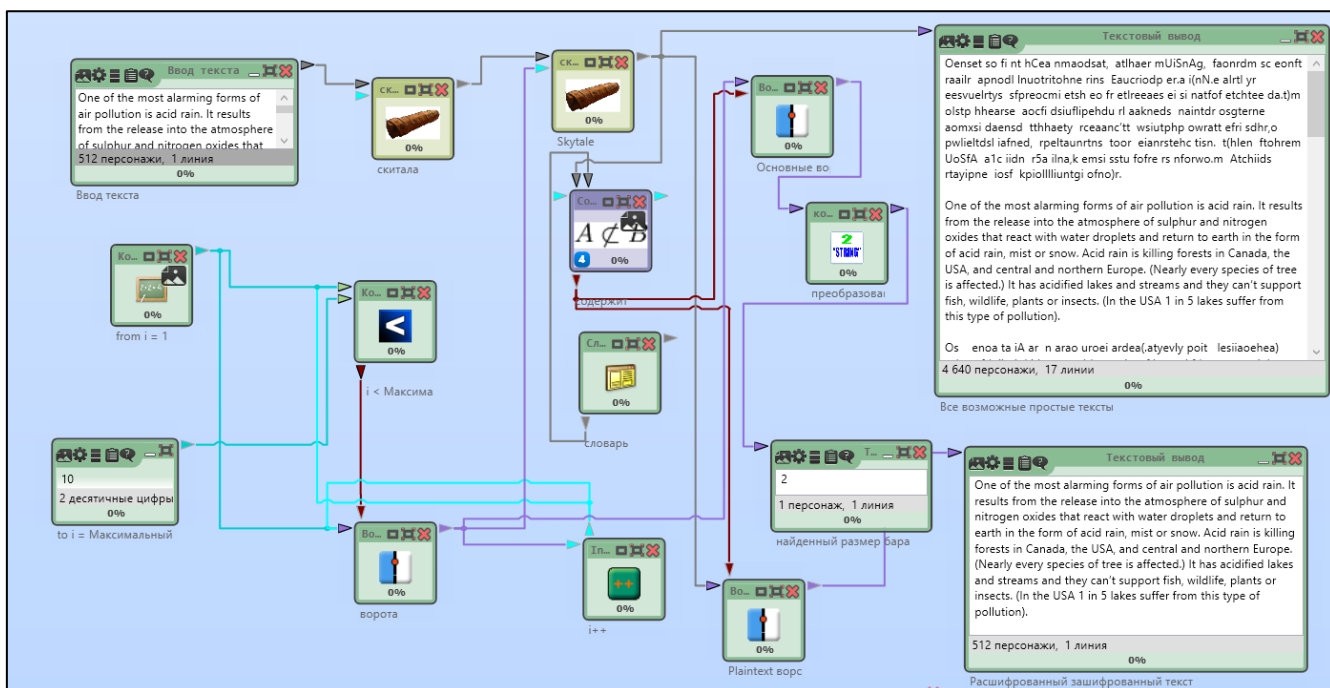


Рисунок 5 – Результат шифрования с помощью Cryptool 2

## Шифр Виженера

### 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 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:
  1. Определите размер ключа с помощью приложения Analysis-> Tools for Analysis-> Autocorrelation
  2. Выполните перестановку текста с размером столбца равным размеру ключа приложением Permutation/Transposition
  3. 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.

## Ход работы

### Реализация в CrypTool 1.0

- Зашифровать и расшифровать текст, содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра с выбранным ключом.

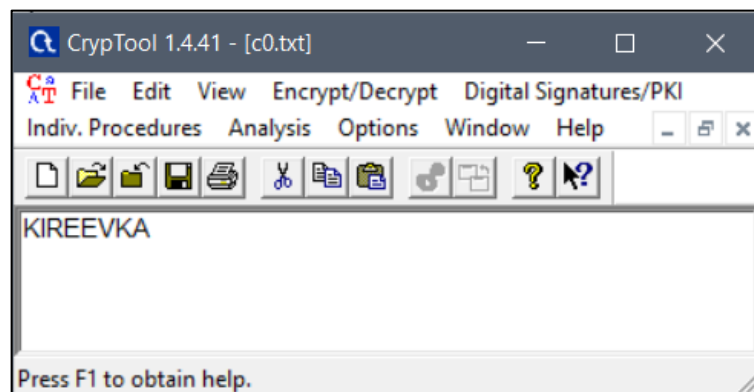


Рисунок 6 – Открытый текст

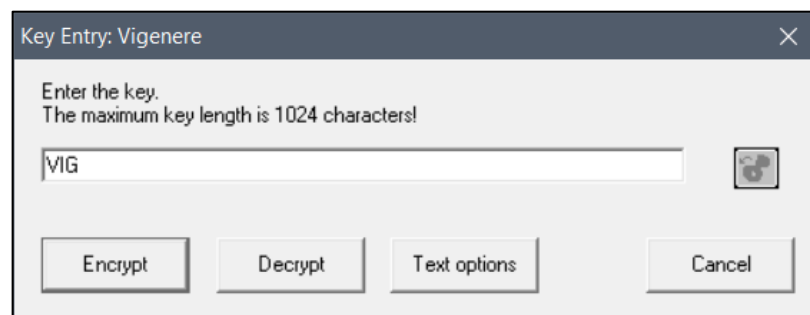


Рисунок 7 – Спецификация параметров

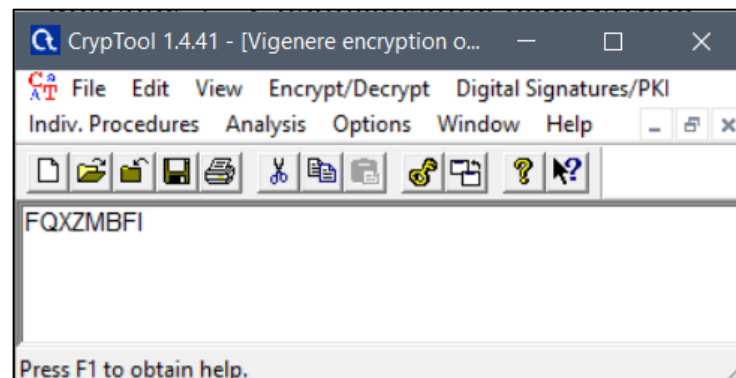


Рисунок 8 – Результат шифрования с помощью программы

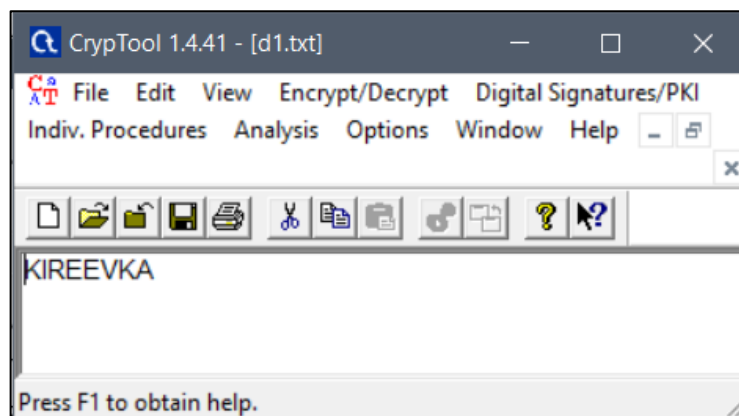


Рисунок 9 – Расшифрованный текст

Результат шифрования вручную:

<i><b>K</b></i>	<i><b>I</b></i>	<i><b>R</b></i>		<i><b>E</b></i>	<i><b>E</b></i>	<i><b>V</b></i>		<i><b>K</b></i>	<i><b>A</b></i>
V	I	G		V	I	G		V	I

A	B	C	D	E	F	G	H	<i><b>I</b></i>	J	<i><b>K</b></i>	L	M	N	O	P	Q	<i><b>R</b></i>	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	A	B	C	D	E	<i><b>F</b></i>	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
I	J	K	L	M	N	O	P	<i><b>Q</b></i>	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

A	B	C	D	<i><b>E</b></i>	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	<i><b>V</b></i>	W	X	Y	Z
V	W	X	Y	<i><b>Z</b></i>	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
I	J	K	L	<i><b>M</b></i>	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	<i><b>B</b></i>	C	D	E	F

A	B	C	D	E	F	G	H	I	J	<i><b>K</b></i>	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	A	B	C	D	E	<i><b>F</b></i>	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
<i><b>I</b></i>	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

Шифротекст: FQXZMBFI

Результаты шифрования вручную и с помощью CrypTool 1.0 совпали.



- Произвести атаку на шифротекст.

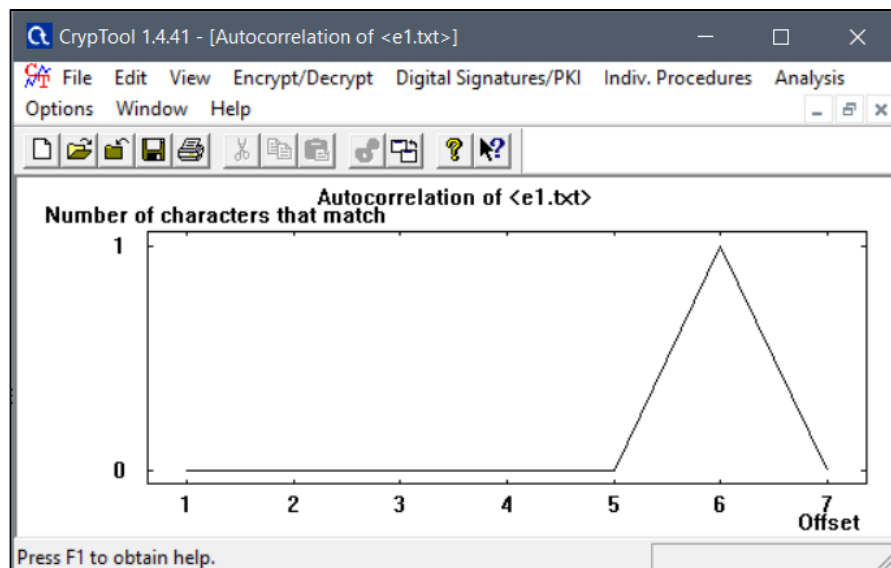


Рисунок 10 – Результат автокорреляции

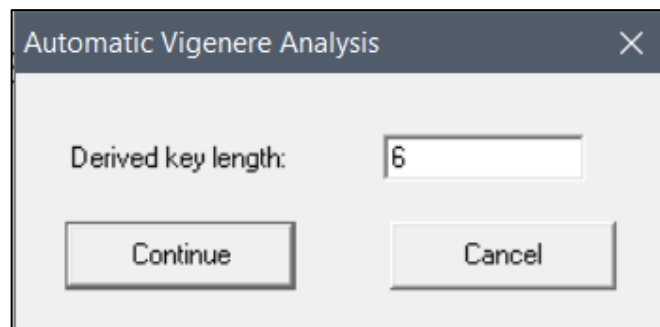


Рисунок 11 – Длина ключа

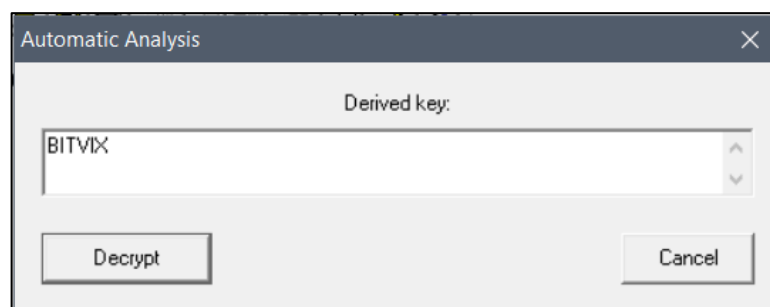
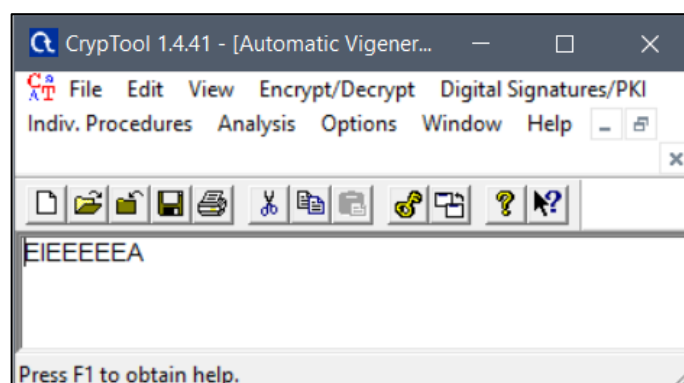


Рисунок 12 – Полученный ключ



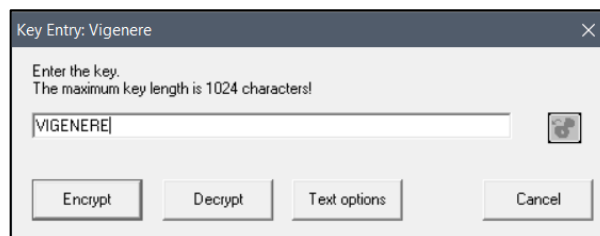
### Рисунок 13 – Расшифрованный текст

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

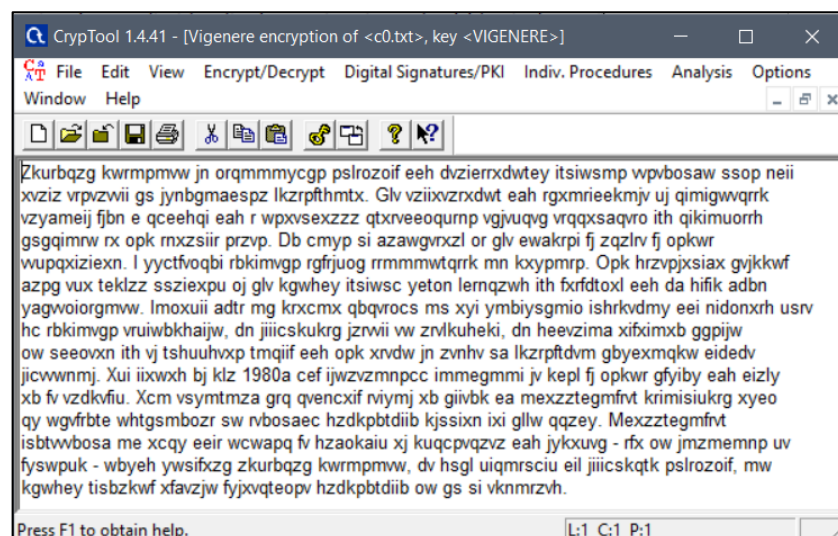
- Повторить атаку для фрагмента текста из файла *English.txt* (папка CrypTool/reference). Размер текста не менее 1000 символов.



### Рисунок 14 – Открытый текст



### Рисунок 15 – Ключ



### Рисунок 16 – Шифротекст

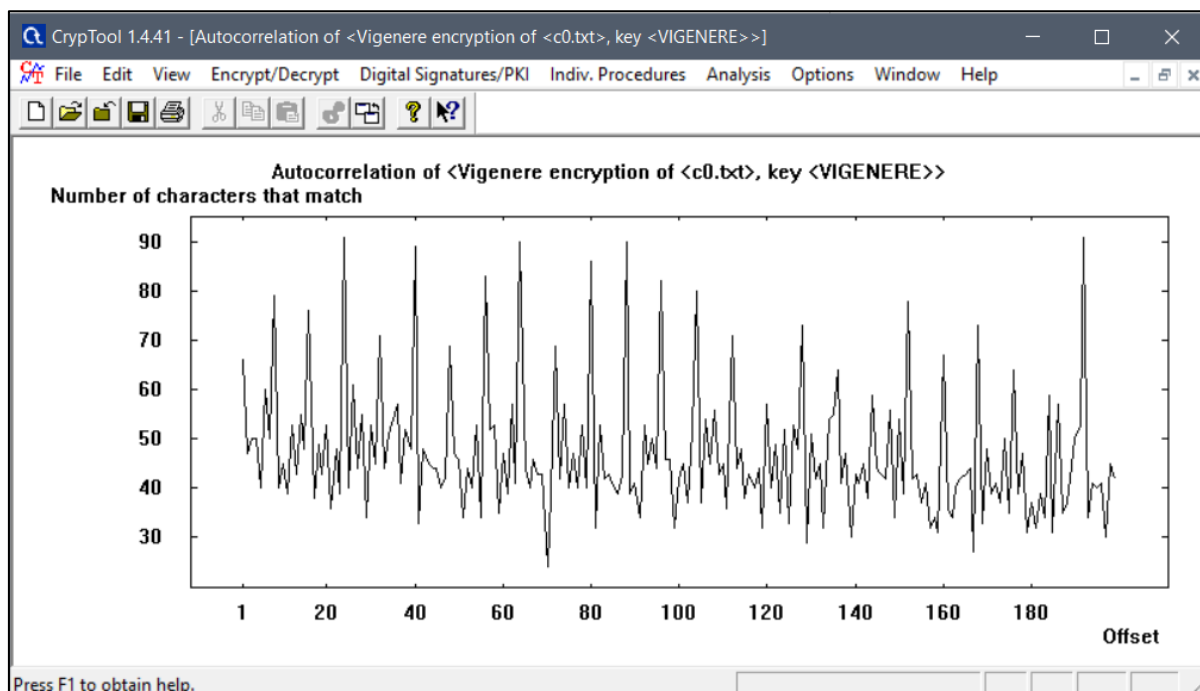


Рисунок 17 – Результат автокорреляции

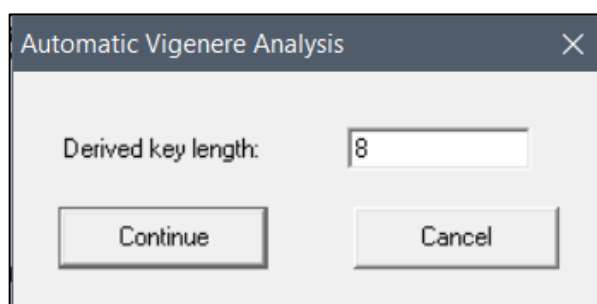


Рисунок 18 – Длина ключа

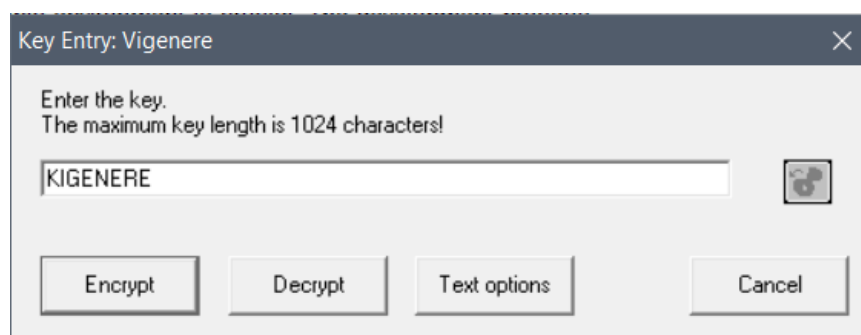


Рисунок 19 – Полученный ключ

Программа правильно распознала длину ключа и сам ключ.

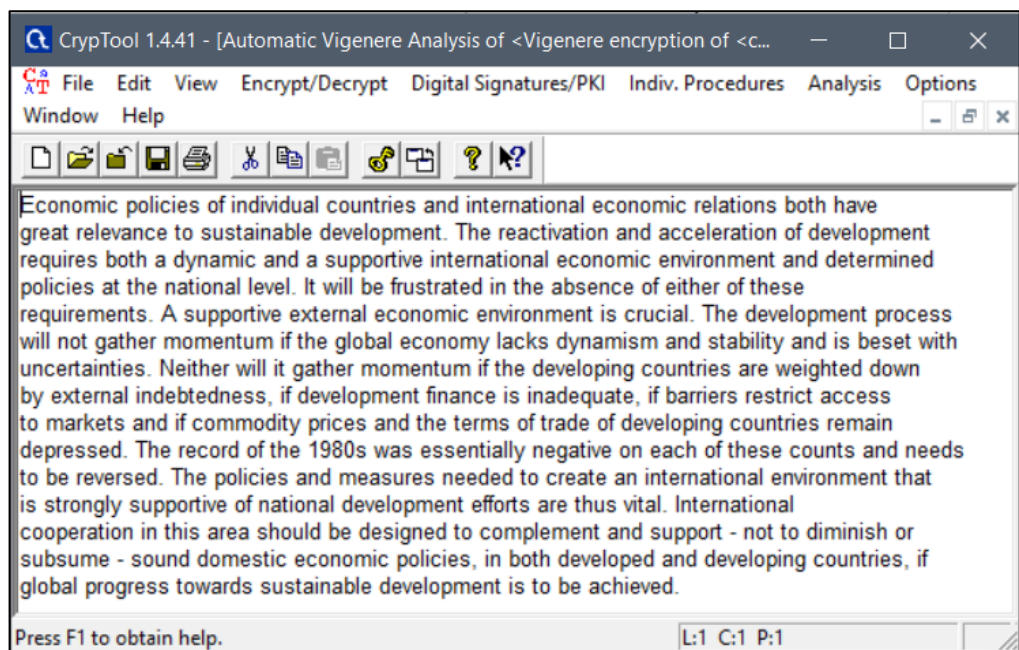


Рисунок 20 – Расшифрованный текст

- Воспроизведите эту атаку в автоматизированном режиме
- Определите размер ключа (8)

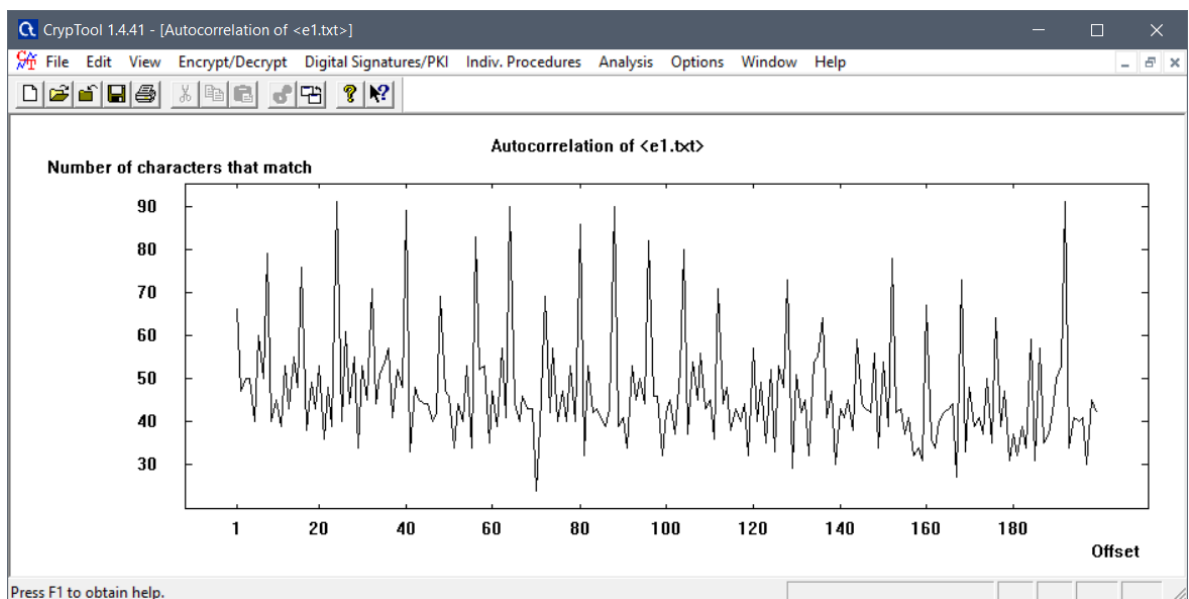


Рисунок 21 – Результат автокорреляции

- Выполните перестановку текста с размером столбца равным размеру ключа

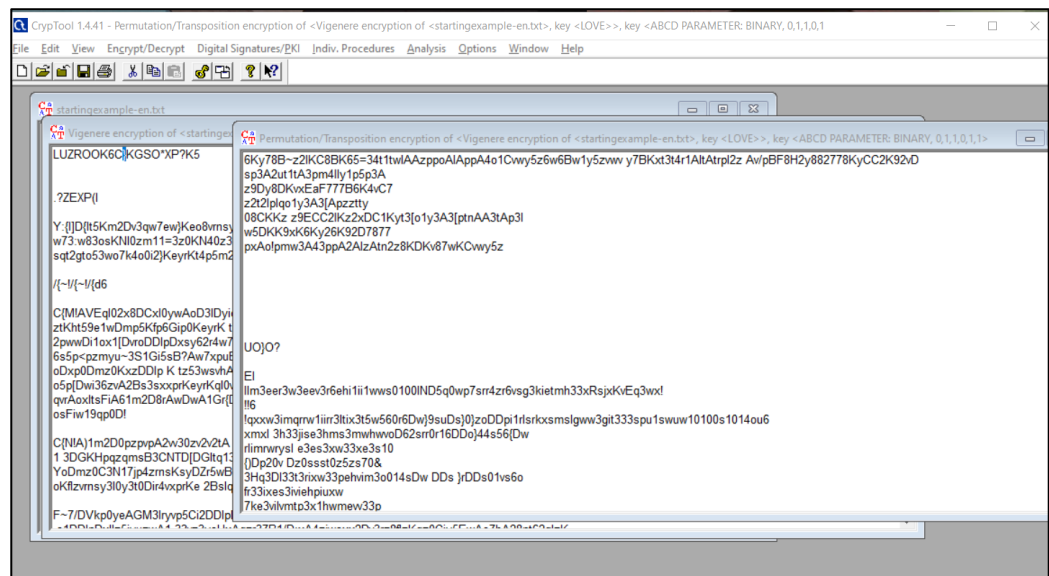


Рисунок 22 – Результат перестановки

Находим 8 алфавитов.

- Определите очередную букву ключа

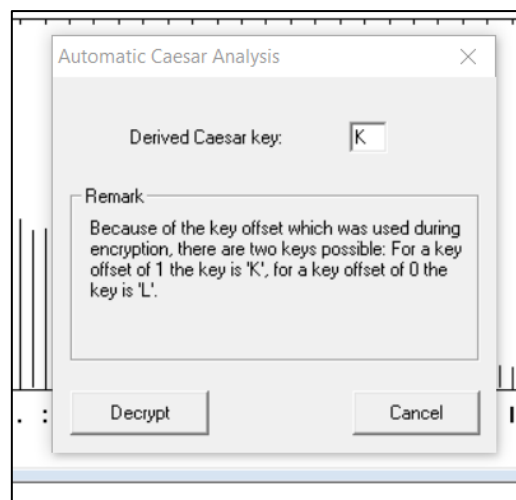


Рисунок 23 – Результат Цезаря

- Самостоятельно изучить атаку, реализованную в CryptTool 2, опираясь на Help и ссылки на статьи.

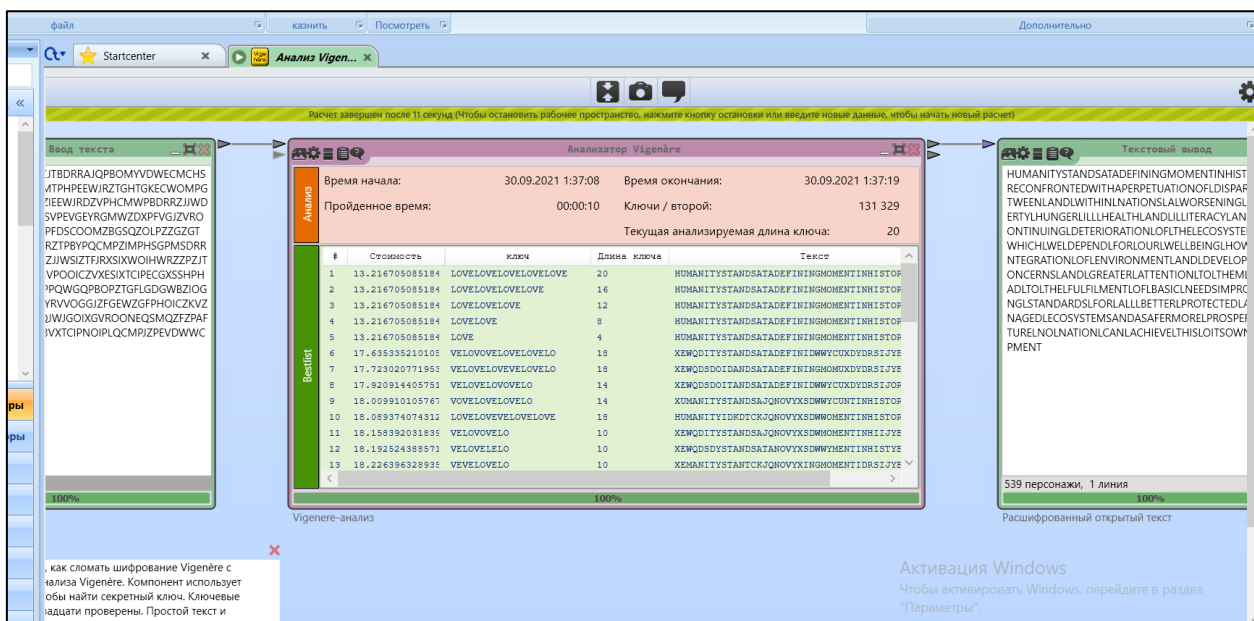


Рисунок 24 – Результат атаки в ScreenshotTool 2.0

### Схема, поясняющая работу шифра

Шифр Виженера - метод полиалфавитного шифрования текста с использованием ключевого слова. Можно рассматривать шифр Виженера состоящим из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая *tabula recta* или квадрат (таблица) Виженера. Выбирается кодовое слово длины  $n$ , которое делит открытый текст на отрезки данной длины. Далее составляется, так называемая, таблица Виженера. Горизонтально записывается алфавит, вертикально под первым символом алфавита записывается кодовое слово. Заполнение таблицы осуществляется символами алфавита, начинающегося с элемента кодового слова, и циклически замыкается (т.е. применительно к латинице это выглядит так: ...xyzabc...). Элемент шифротекста выбирается на пересечении столбца, соответствующего букве открытого текста и строки, соответствующей букве кодового слова.

Например, зашифруем текст «ПРИМЕРШИФРАВИЖЕНЕРА», используя кодовое слово «КЛЮЧ» и русский алфавит:

1. Делим текст на отрезки:

п	р	н	м	е	р	ш	н	ф	р	а	в	н	ж	е	н	е	р	а	
к	л	ю	ч	к	л	ю	ч	к	л	ю	ч	к	л	ю	ч	к	л	ю	

2. Производим замену (для 1ого отрезка):

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
К	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	а
Л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	к
Ю	я	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
Ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц

Получаем шифротекст для первого отрезка: *ШЪЖВ*

3. Производим аналогичную замену всех отрезков, получаем итоговый шифротекст: *ШЪЖВПЪЦЯЭЪЮЦТСГПЪЮ*

### **Тип шифра**

Тип шифра – замена.

### **Ключ шифра**

Ключ шифра – ключевое слово.

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

При длине алфавита  $n$  и длине ключевого слова  $m$  сложность атаки “грубой силы”  $n! / (n-m)!$

### **Описание выполненной процедуры атаки на шифротекст**

Сначала необходимо узнать длину ключа с помощью автокорреляционного метода. Далее с помощью статистического метода находят ключ. Для этого шифротекст разделяем на блоки одного алфавита. После этого применяем к каждому блоку анализ Caesar, узнаем возможный символ заданного алфавита

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

- Первый шаг – выбирается случайный ключ, производится дешифровка с его использованием

- Ключ изменяется, и для него рассчитывается “стоимость” – метрика, характеризующая полезность примененных изменений
- Если изменение полезно, оно сохраняется, предпринимается дальнейшая попытка улучшить ключ
- Шаги 2-3 повторяются до тех пор, пока ключ не станет нельзя улучшить

## **Шифр Хилла**

### **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 выбранным ключом 2x2. Убедиться в совпадении результатов. Проверить обратимость шифрующей матрицы (ключа).
3. Зашифровать текст с произвольным сообщением в формате «DEAR MR ФАМИЛИЯ ИМЯ ОТЧЕСТВО THANK YOU VERY MUCH», используя транслитерацию латиницей и шифрующую матрицу 3x3.
4. Выполнить атаку на основе знания открытого текста, используя приложение из Analysis-> Symmetric Encryption(classic)-> Known Plaintext.
5. Удалить из сообщения и шифротекста фрагменты с ФАМИЛИЯ ИМЯ ОТЧЕСТВО и повторить атаку. Убедиться, что полученный ключ (матрица) совпадает с исходным.
6. Передайте произвольную шифровку коллеге для расшифрования при условии, что формы обращения и завершения сообщения известны. Размер использованного ключа держать в секрете.



## Ход работы

### *Исходное описание шифра, пример вычисления шифрующей и расшифровывающей матрицы*


Шифр Хилла основан на матричном преобразовании текста. Перед шифрованием необходимо каждому символу алфавита следует сопоставить код равный порядковому номеру символа в алфавите. Затем коды символов открытого текста записываются в матрицу размера  $n \times m$  и создается шифрующая матрица  $n \times n$ . Для шифрования производится умножение матрицы открытого текста на шифрующую матрицу и вычисляется остаток от деления значения элементов матрицы-произведения на число символов выбранного алфавита. Для расшифровки необходимо шифротекст умножить на матрицу, которая является мультипликативной инверсией по отношению к шифрующей для выбранного алфавита.

### Шифр Хилла : зашифрование (1929)

➤ **Открытый текст:**  
HILLCIPHEREXAMPLES


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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

7	8	11
11	2	8
15	7	4
17	4	23
0	12	15
11	4	18



6	24	1
13	16	10
20	17	15

Шифрующая матрица



366	483	252
252	432	151
261	540	145
614	863	402
456	447	345
478	634	321



2	15	18
18	16	21
1	20	15
16	5	12
14	5	7
10	10	9

(mod 26)

➤ **Шифротекст:**  
CPSSQVBUPQFMOFHKKJ

## Шифр Хилла: расшифрование<sup>(1929)</sup>

➤ Шифротекст:

CPSSQVBUPQFMOFHKKJ

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2	15	18
18	16	21
1	20	15
16	5	12
14	5	7
10	10	9



8	5	10
21	8	21
21	12	8

Дешифрующая  
матрица  
(обратная)



709	346	479
921	470	684
743	345	550
485	264	361
364	194	301
479	238	382



7	8	11
11	2	8
15	7	4
17	4	23
0	12	15
11	4	18

(mod 26)

➤ Открытый текст:

HILLCIPHEREXAMPLES

## Шифр Хилла: свойства шифрующей матрицы

- В общем случае матрица шифрования квадратная  $m \times m$ , где  $m$  – размер блока текста, подлежащего зашифрованию
- Матрица обратима в том и только в том случае, когда ее детерминант не равен нулю и не имеет общих делителей с основанием модуля
- Обратная матрица  $M^{-1}$  является мультипликативной инверсией  $M$  в  $\mathbb{Z}_{26}$  (см. «Модульная арифметика»)

- Шифр не сохраняет статистику обычного текста
- Возможна атака на ключ на основе знания исходного текста:
  - Делается предположение о размере блока  $m$
  - Добываются не менее  $m$  пар блоков открытого текста и шифротекста и строится уравнение  $C = P \times K$
  - Выполняется попытка восстановить матрицу-ключ  $K = C \times P^{-1}$
  - В случае неудачи выбирается другой размер блока  $m$

### Реализация в CrypTool 1.0

- Зашифровать и расшифровать текст содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра с выбранным ключом 2x2.

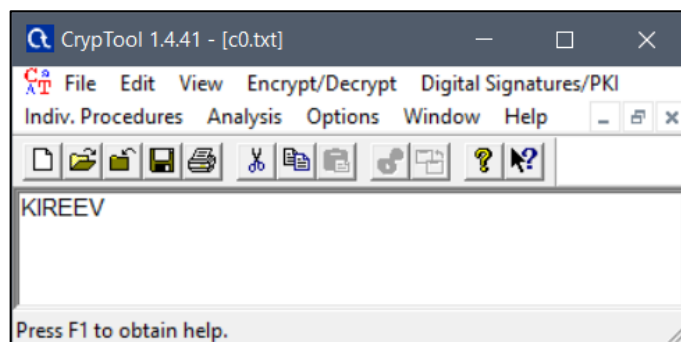


Рисунок 24 – Открытый текст

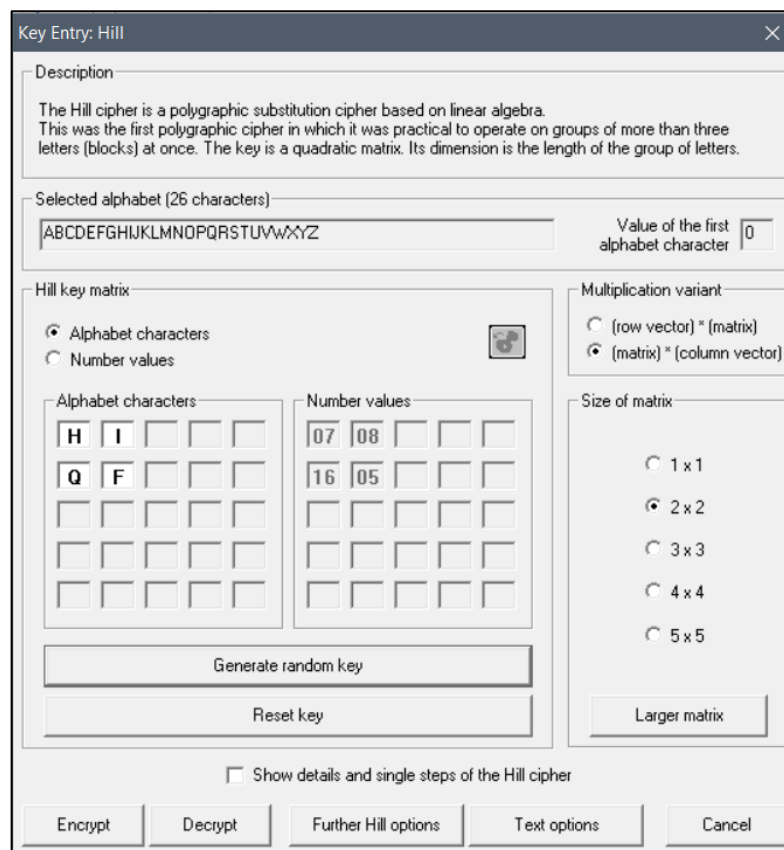


Рисунок 25 – Спецификация параметров

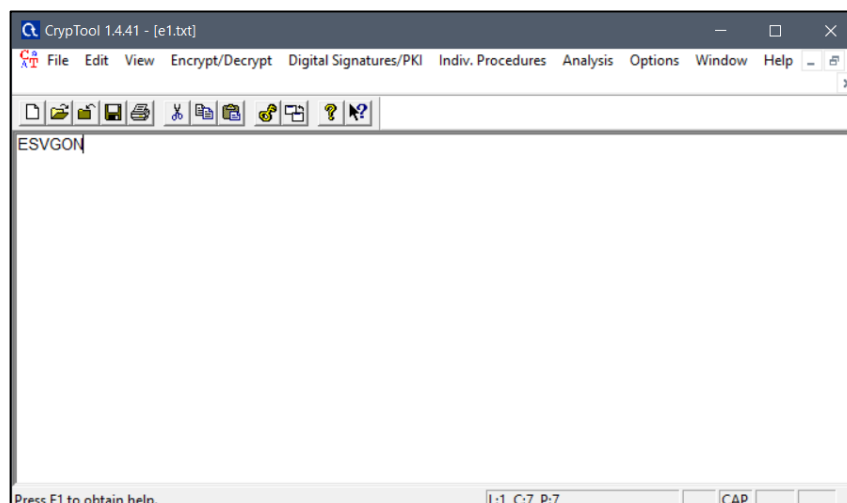


Рисунок 26 – Результат шифрования с помощью программы

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Матрица для открытого текста:

10	8
17	4
4	21

Ключ:

7	8
16	5

Определитель матрицы  $-93$ , следовательно обратная матрица существует.

Перемножим матрицы:

134	200
151	292
196	169

Возьмем полученную матрицу по модулю 26:

4	18
21	6
14	13

Шифротекст: ESVGON

Дешифрующая матрица:

17	4
8	3

Перемножим матрицы:

212	70
405	102
304	231

Возьмем полученную матрицу по модулю 26:

10	8
17	4
4	21

Полученный открытый текст совпадает с исходным.

- Зашифровать текст с произвольным сообщением в формате «DEAR MR ФАМИЛИЯ ИМЯ ОТЧЕСТВО THANK YOU VERY MUCH», используя транслитерацию латиницей и шифрующую матрицу 3x3.

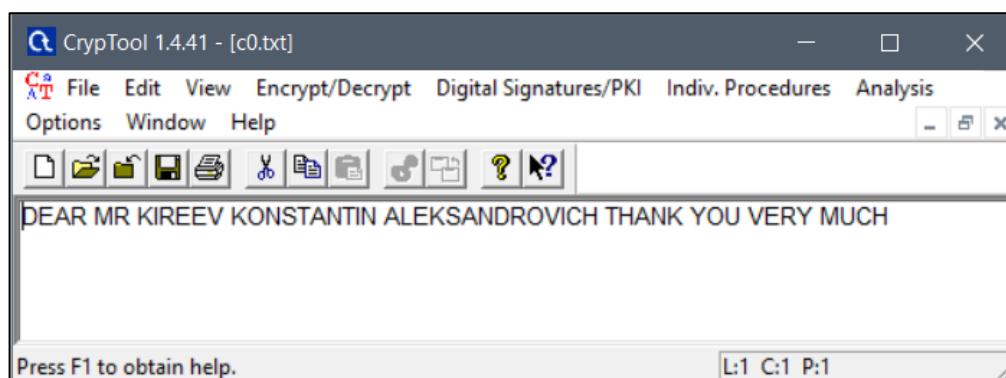


Рисунок 27 – Открытый текст

**Key Entry: Hill**

**Description**  
The Hill cipher is a polygraphic substitution cipher based on linear algebra. This was the first polygraphic cipher in which it was practical to operate on groups of more than three letters (blocks) at once. The key is a quadratic matrix. Its dimension is the length of the group of letters.

**Selected alphabet (26 characters)**  

Value of the first alphabet character

**Hill key matrix**  
☒ Alphabet characters  
☐ Number values

Alphabet characters					Number values				
T	B	D			19	01	03		
C	W	V			02	22	21		
W	R	Q			22	17	16		

Generate random key  
Reset key

**Multiplication variant**  
☐ (row vector) \* (matrix)  
☒ (matrix) \* (column vector)

**Size of matrix**  
☐ 1 x 1  
☐ 2 x 2  
☒ 3 x 3  
☐ 4 x 4  
☐ 5 x 5

Larger matrix

☐ Show details and single steps of the Hill cipher

Encrypt Decrypt Further Hill options Text options Cancel

Рисунок 28 – Спецификация параметров

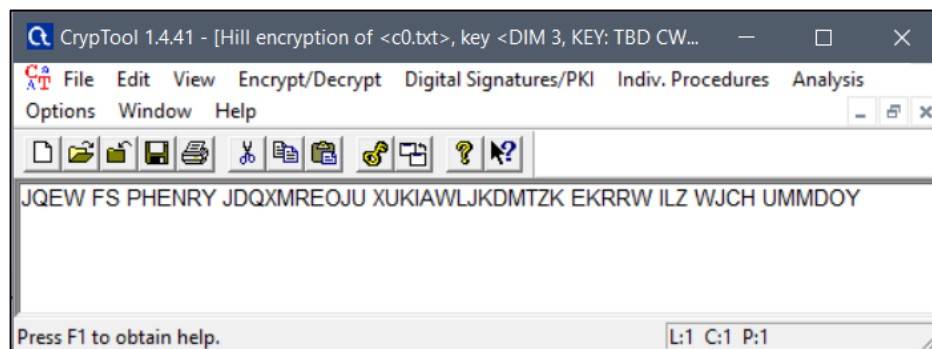


Рисунок 29 – Результат шифрования с помощью программы

- Выполнить атаку на основе знания открытого текста, используя приложение из Analysis-> Symmetric Encryption(classic)-> Known Plaintext.

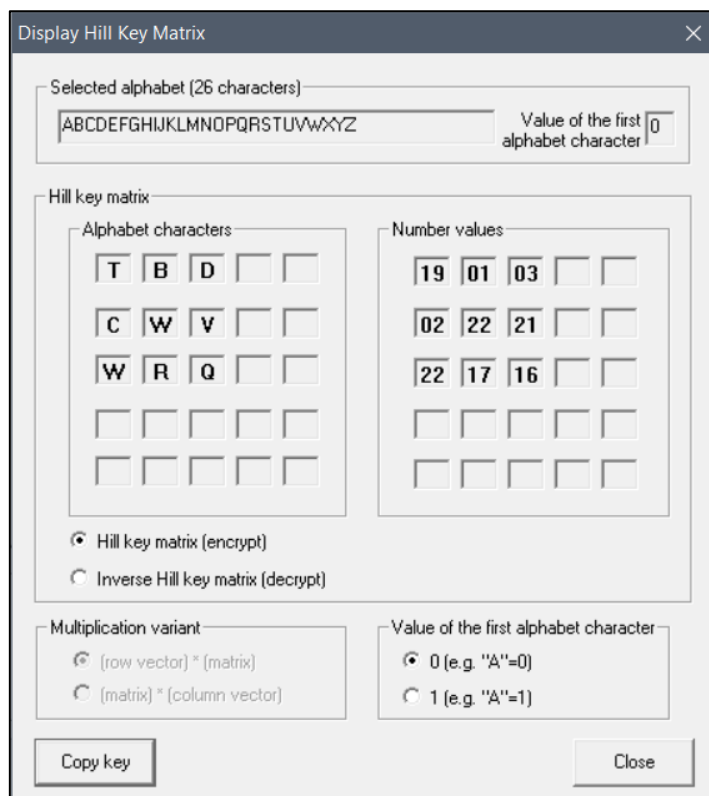


Рисунок 30 – Спецификация параметров

- Удалить из сообщения и шифротекста фрагменты с ФАМИЛИЯ ИМЯ ОТЧЕСТВО и повторить атаку. Убедиться, что полученный ключ (матрица) совпадает с исходным.

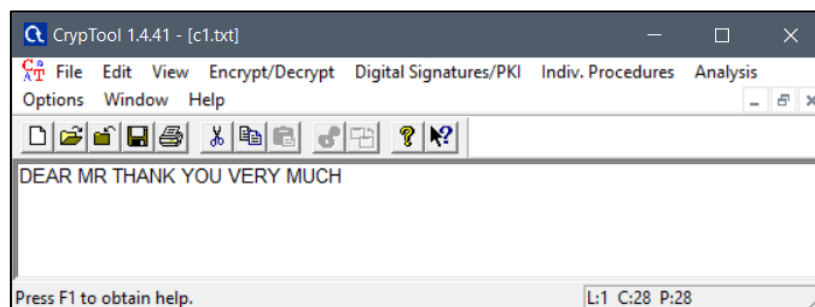


Рисунок 31 – Открытый текст

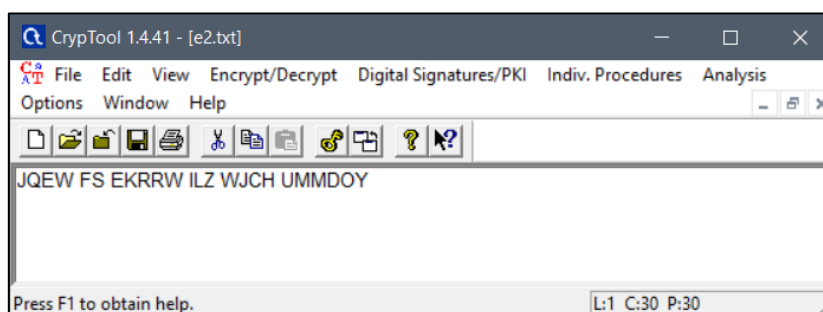


Рисунок 32 – Шифротекст

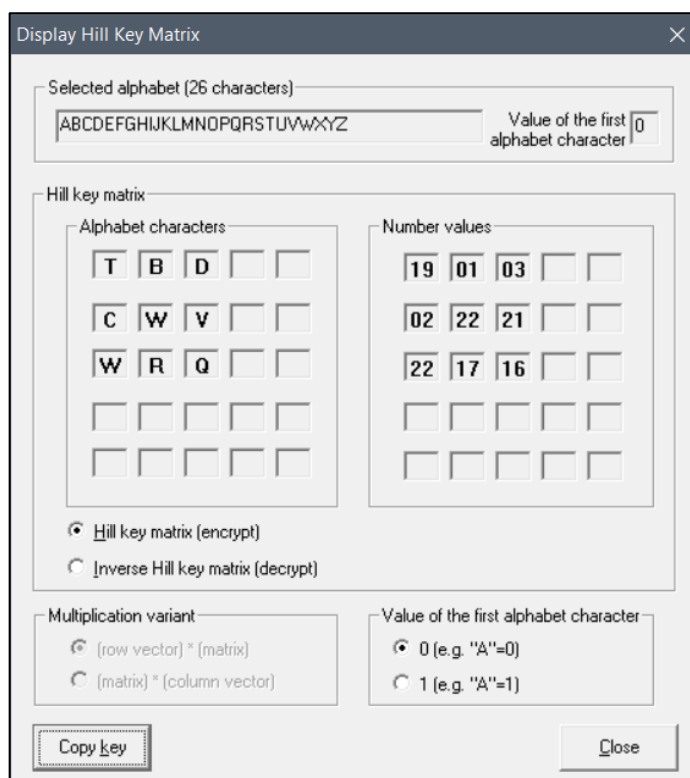


Рисунок 33 – Полученный ключ

Полученный ключ (матрица) совпадает с исходным.

- Передайте произвольную шифровку коллеге для расшифрования при условии, что формы обращения и завершения сообщения известны. Размер использованного ключа держать в секрете.

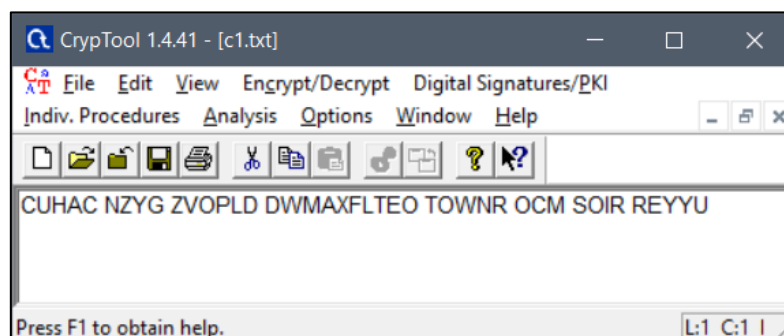


Рисунок 34 – Шифротекст

Открытый текст начинается с HELLO DEAR FRIEND и заканчивается MUCH BYE.

Удалим неизвестную часть.



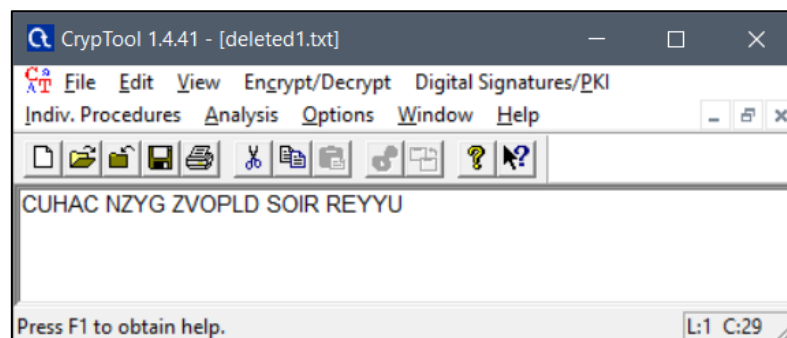


Рисунок 35 – Модифицированный шифротекст

Выполним атаку на основе открытого текста.

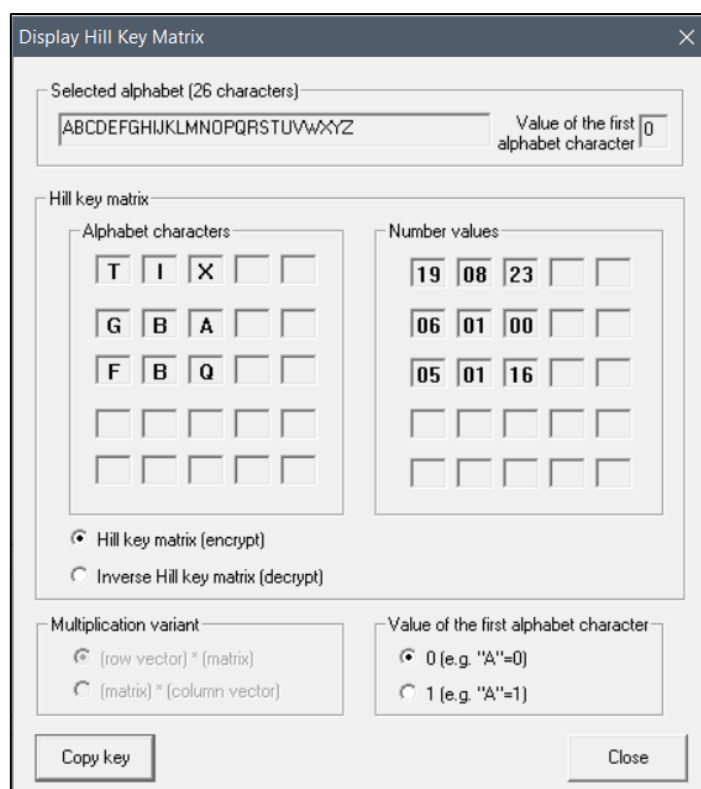


Рисунок 36 – Полученный ключ

Дешифруем полученное сообщение.

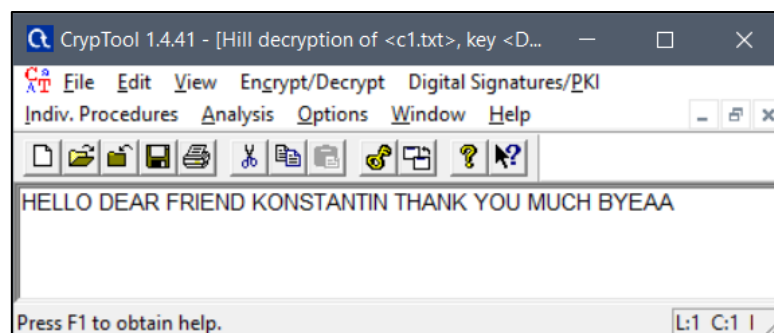


Рисунок 37 – Дешифрованное сообщение

***Тип шифра***

Тип шифра – замена, блочный.

***Ключ шифра***

Ключ шифра – шифрующая матрица.

***Оценка сложности атаки «грубой силы»***

Сложность атаки методом «грубой силы» в худшем случае  $n^{m \cdot m}$ .

## Выводы

	Scytale	Vigenere	Hill
Тип	Перестановка	Замена	Замена, блочный
Ключ	Количество граней и смещение	Последовательность символов (ключевое слово)	Шифрующая матрица
Оценка сложности атаки “грубой силы”	При количестве граней $n$ ключ можно подобрать за $n^2$ шагов	При длине алфавита $n$ и длине ключевого слова $m$ сложность атаки “грубой силы” $\frac{n!}{(n-m)!}$	Сложность атаки методом «грубой силы» в худшем случае $n^{m \times m}$
Описание	Прибор состоит из гранёного цилиндра (жезла) и узкой полоски пергамента, которая обматывается вокруг цилиндра по спирали. На гранях цилиндра записывалось сообщение.	Выбирается кодовое слово длины $n$ , которое делит открытый текст на отрезки данной длины, составляется таблица Виженера. Элемент шифротекста выбирается на пересечении столбца, соответствующего букве открытого текста и строки, соответствующей букве кодового слова.	Коды символов открытого текста записываются в матрицу размера $n \times m$ и создается шифрующая матрица $n \times n$ . Для шифрования производится умножение матрицы открытого текста на шифрующую матрицу и вычисляется остаток от деления значения элементов матрицы-произведения на число символов выбранного алфавита.
Математическая формула	$index =  m * (i \bmod n)  +  i \div n $	$c_j = (m_j + k_j) \bmod n$	$C = (A * B) \bmod n$