МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра информационной безопасности

ОТЧЕТ

по практической работе №1
по дисциплине «Криптографические методы защиты информации»
Тема: «Изучение классических шифров Scytale, Vigenere, Hill»
Вариант 6

Студент гр. 9361 _____ Кисляков Н.

Преподаватель _____ Племянников А.К.

Санкт-Петербург
2023

Цель работы

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

1. Шифр «Сцитала» (Scytale)

1.1 Задание

1. Найти шифр в CrypTool 1: Encrypt/Decrypt –> Symmetric(Classic) Scytal/Rail Fence.

На рисунке 1 был найден шифр Scytal/Rail Fence в CrypTool 1.

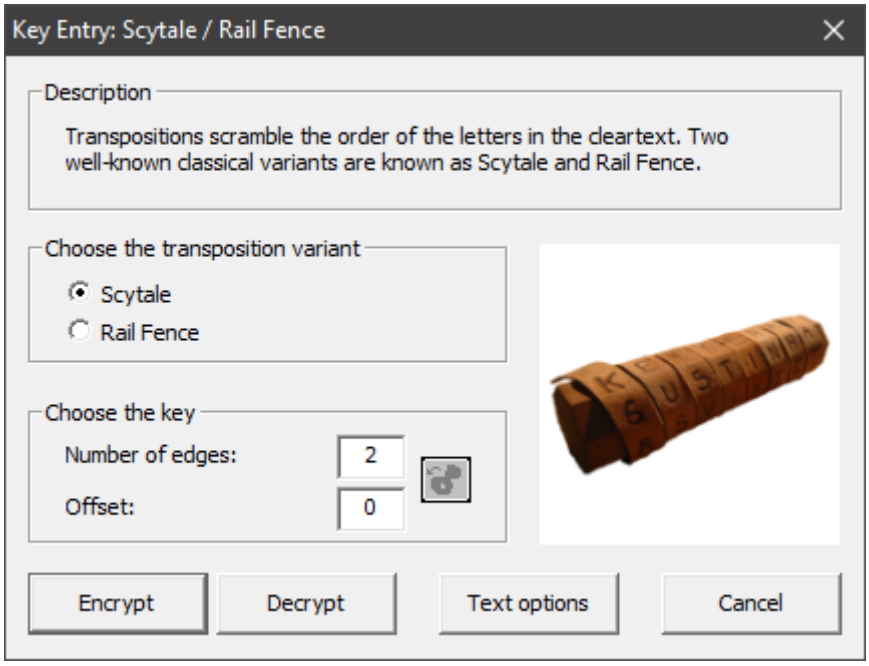

Рисунок 1 – Шифр Scytal/Rail Fence в CrypTool 1

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

На рисунке 2 был создан файл с последовательностью цифр «123456789».

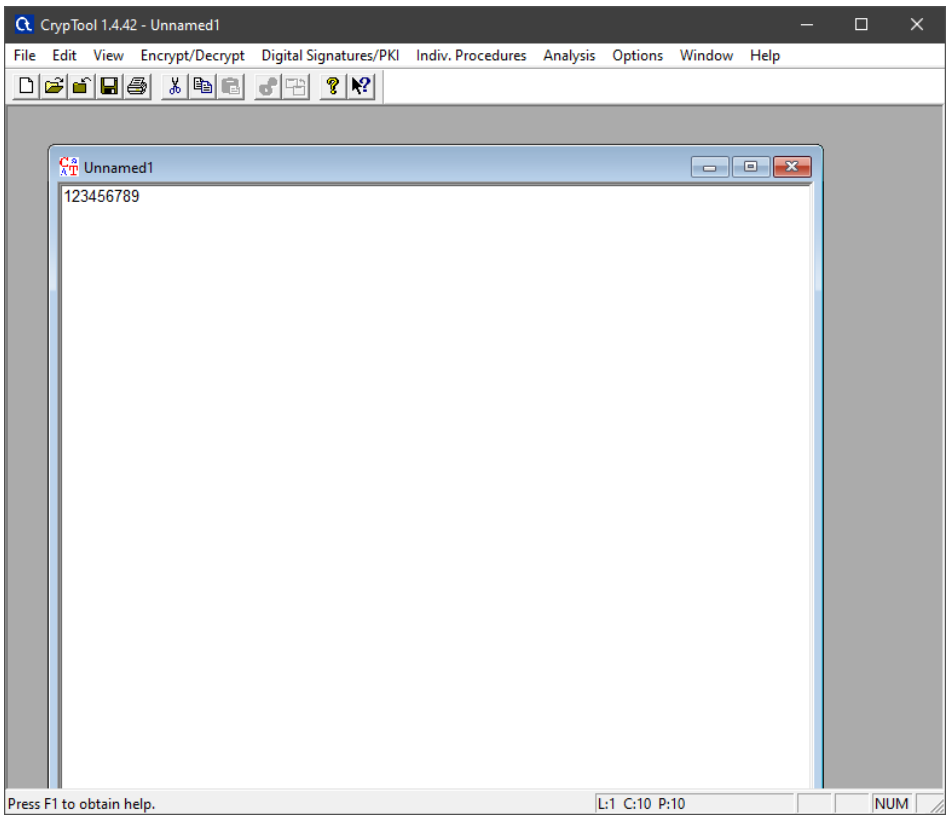

Рисунок 2 – Последовательность цифр

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

На рисунке 3 представлена зашифровка с помочью шифра Scytal/Rail.

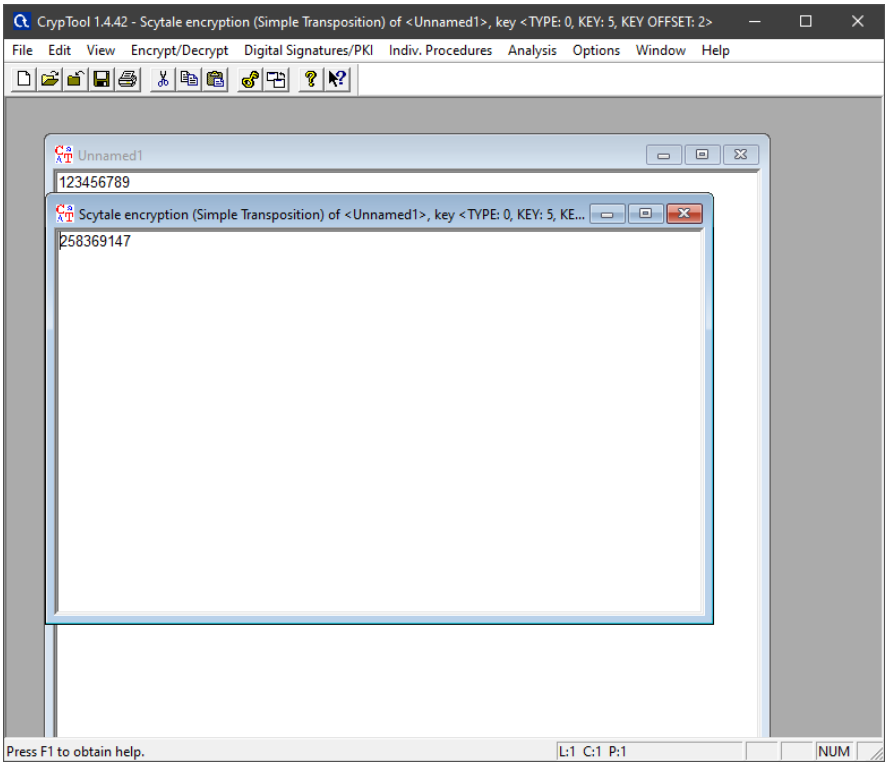

Рисунок 3 – Зашифровка

На рисунке 4 представлена расшифровка с помочью шифра Scytal/Rail.

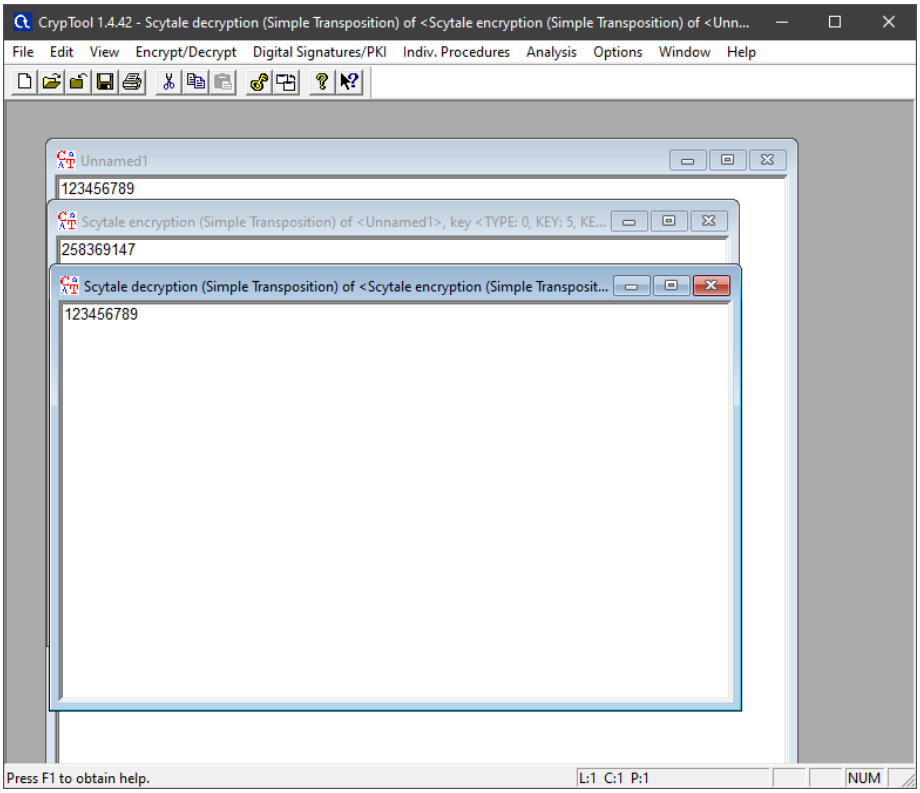

Рисунок 4 – Расшифровка

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

Пусть Number of Edges=4 и Offset=2. При использовании шифра Scytal/Rail, мы получили таблицу №1. В итоге получаем зашифрованный текст «258369147».

Таблица №1

–	–	1
2	3	4
5	6	7
8	9	

Пусть Number of Edges=5 и Offset=1. При использовании шифра Scytal/Rail, мы получили таблицу №1. В итоге получаем зашифрованный текст «246813579».

Таблица №2

–	1
2	3
4	5
6	7
8	9

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.

Исходные данные: входной текст «kisliakov», Number of Edges=5 и Offset=3. Продемонстрируем шифр в виде таблицы 3 и получили зашифрованный текст «ilaoksikv».

Таблица №3

–	–
–	k
i	s
l	i
a	k
o	v

На рисунке 5 показана зашифровка текста «kisliakov» с помочью шифра Scytal/Rail.

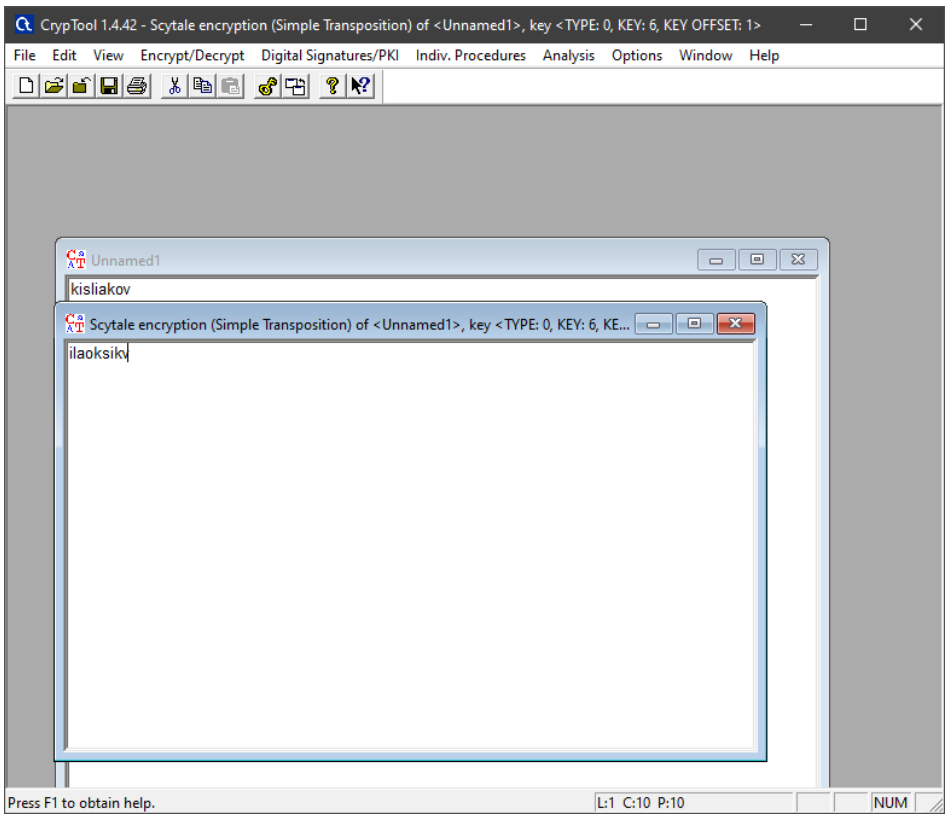

Рисунок 5 – Зашифровка

На рисунке 6 показана расшифровка текста «kilaoksikv» с помочью шифра Scytal/Rail.

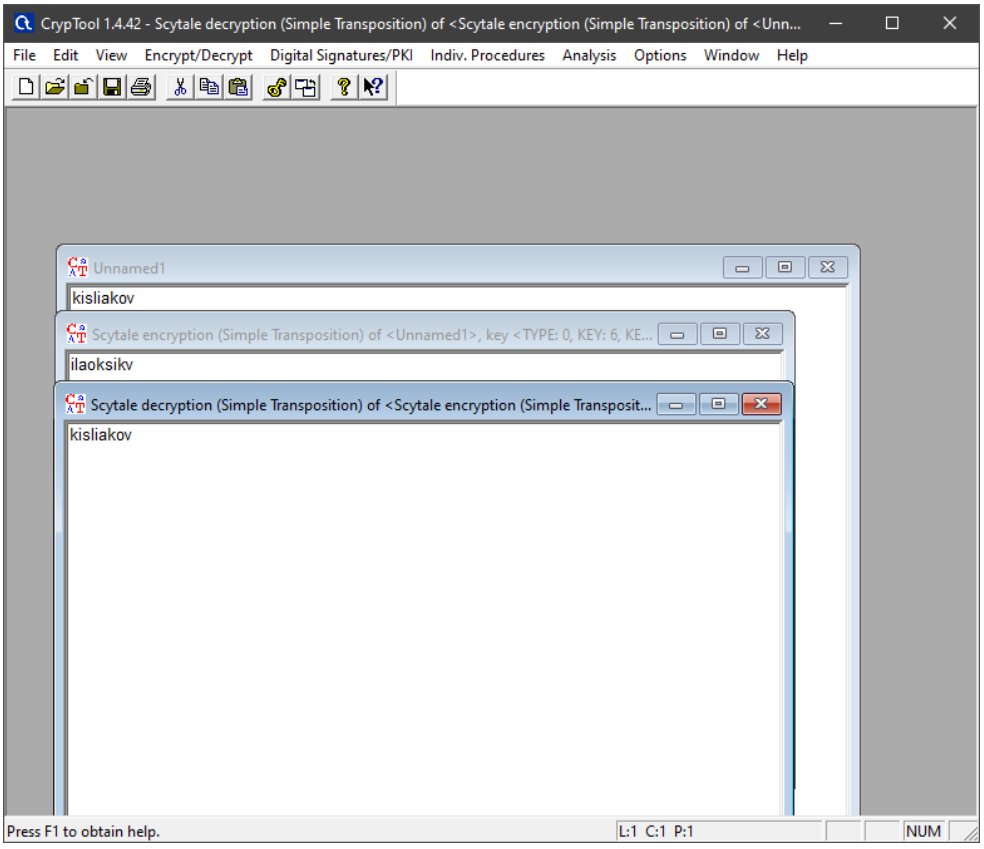

Рисунок 6 – Расшифровка

6. Выполнить самостоятельную работу: взять в CrypTool 2 шаблон атаки на шифр методом «грубой силы» и модифицировать это шаблон, заменив блок с шифротекстом на блок ввода открытого текста и блок зашифрования. Изучить принципы этой автоматической атаки.

На рисунке 7 представлен шаблон атаки на шифр методом «грубой силы» в CrypTool 2.

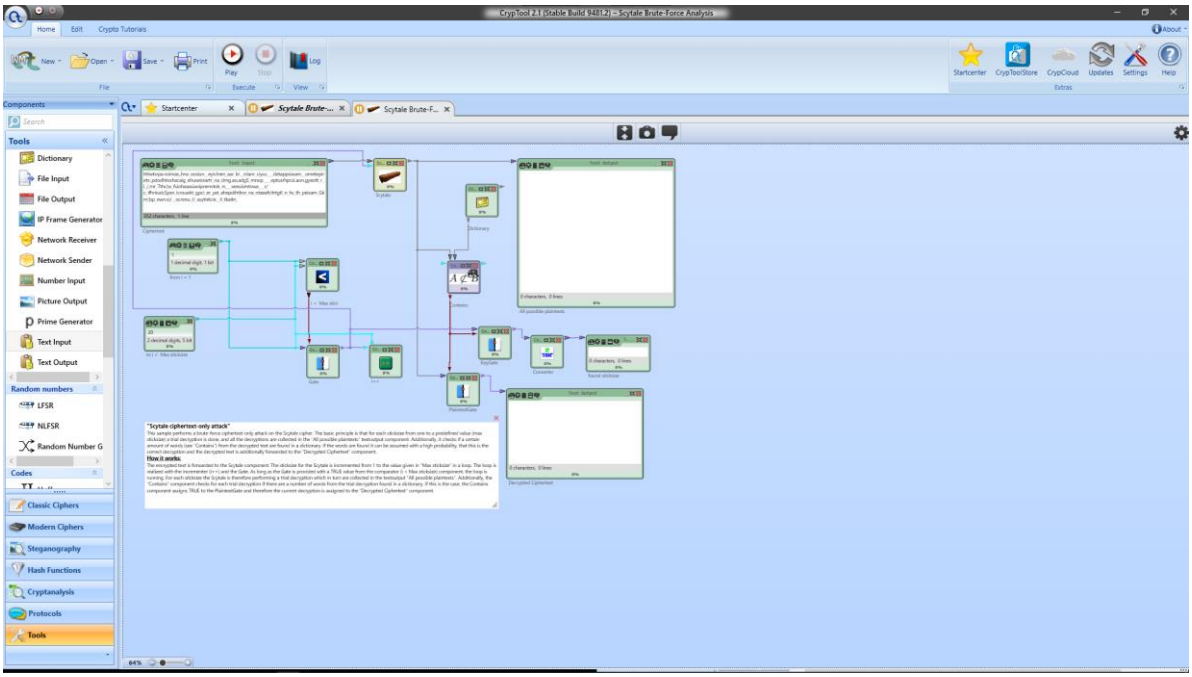

Рисунок 7 – Шаблон

На рисунке 8 представлен модифицированный шаблон атаки на шифр методом «грубой силы» в CrypTool 2.

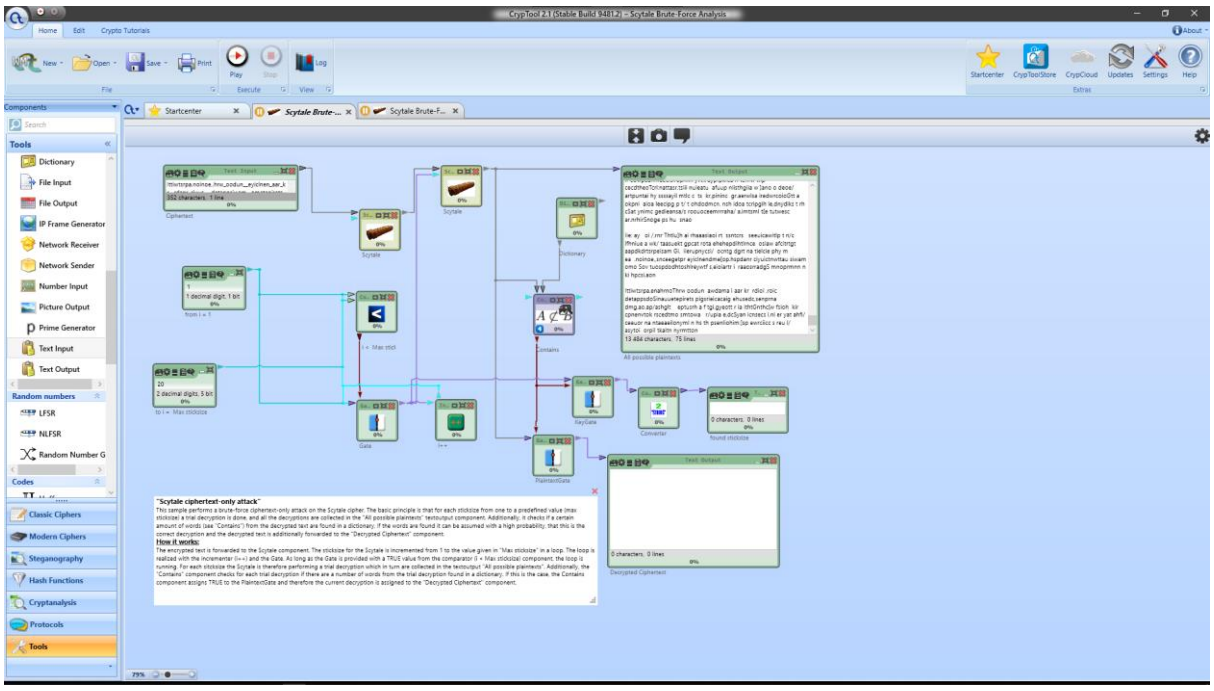

Рисунок 8 – Шаблон

1.2 Реализация в CrypTool 1 (скриншот, спецификация параметров).

Шифр «Сцитала» (Scytale) в CrypTool 1 представлен на рисунке 9, в данном шифре необходимо указать количество ребер смещение.

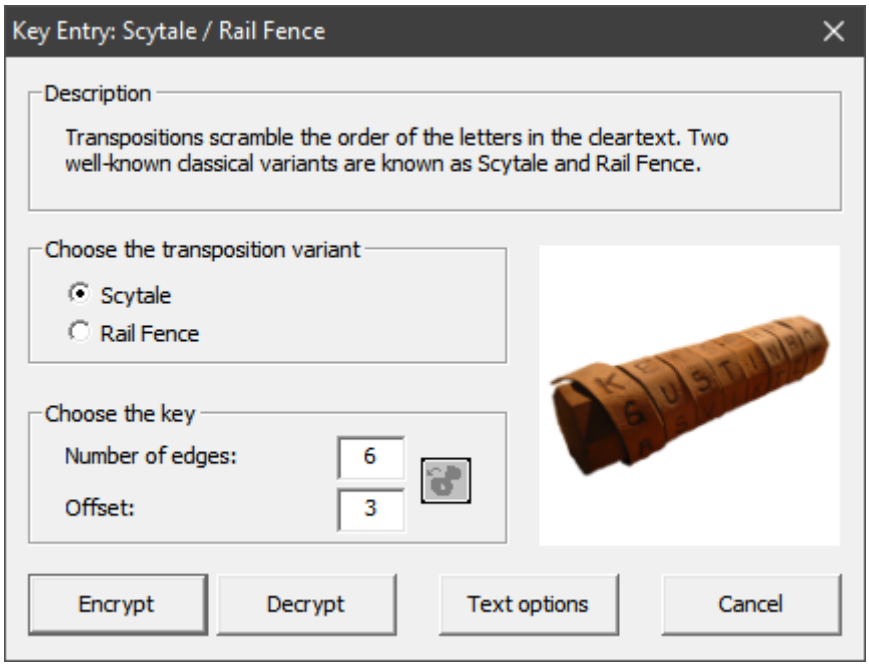

Рисунок 9 – Шифр «Сцитала»

1.3 Схема, поясняющая работу шифра.

На рисунке 10 представлена схема шифра «Сцитала».

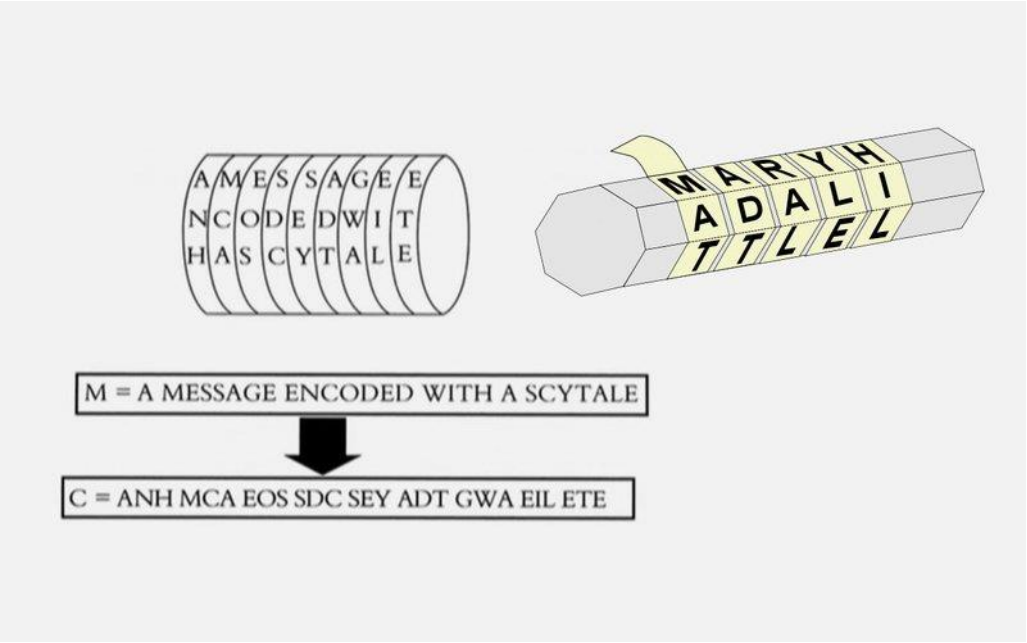

Рисунок 10 – Схема шифра «Сцитала»

1.4 Пример работы шифра для выбранных параметров.

Исходные данные: входной текст «kisliakov», Number of Edges=5 и Offset=3. На рисунке 11 показана зашифровка текста «kisliakov» с помочью шифра Scytal/Rail.

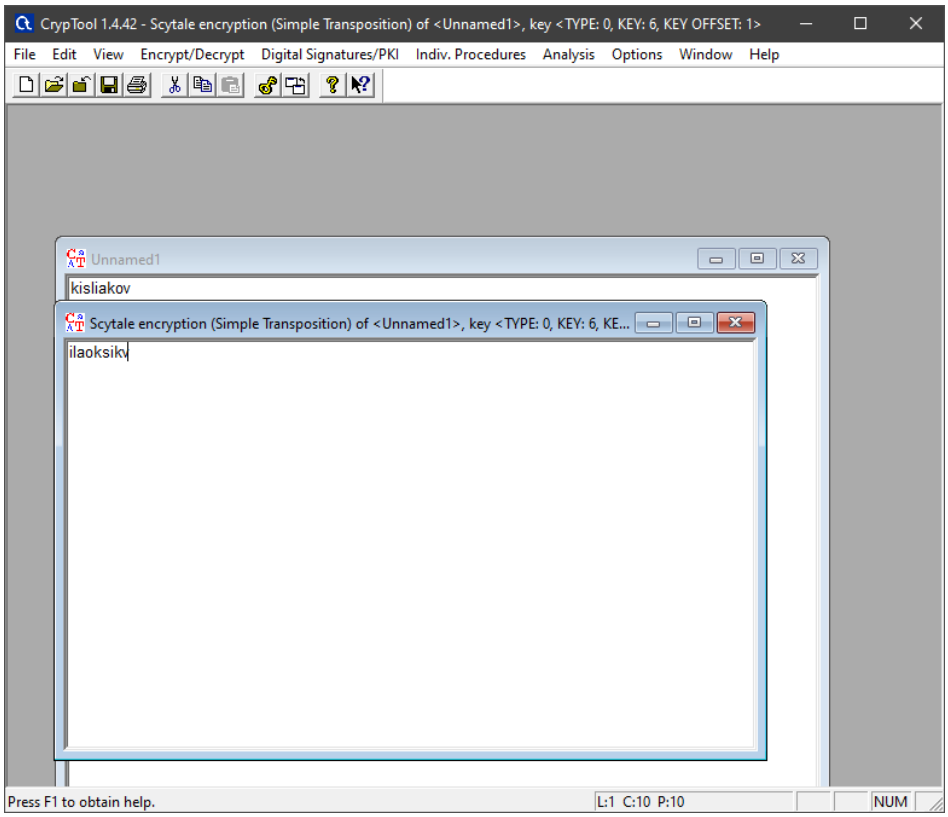

Рисунок 11 – Пример работы шифра

1.5 Основные характеристики шифра:

а) тип шифра (перестановка, замена, комбинированный);

Тип шифра: перестановка.

б) ключ шифра;

Ключ шифра: количество рёбер и размер смещения.

в) оценка сложности атаки «грубой силы».

Сложность атаки «грубой силы»: $O(n^2)$.

2. Шифр Виженера (Vigenere)

2.1 Задание.

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

На рисунке 12 нашли шифр в CrypTool 1.

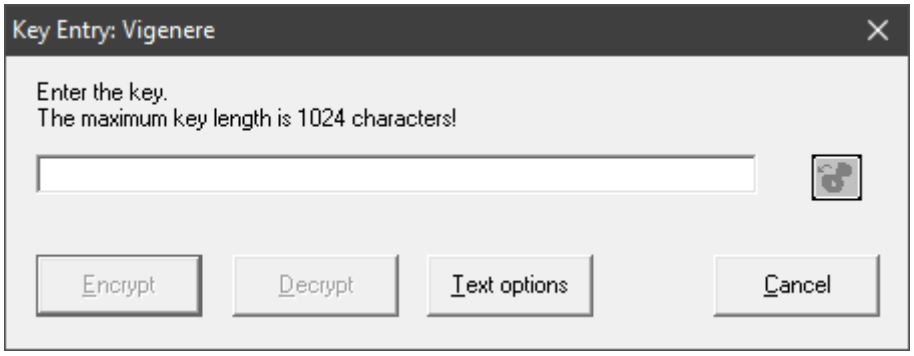

Рисунок 12 – Пример работы шифра

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

Зашифруем тест «KISLIAKOV» с помощью ключа KEY в таблице 4.

Таблица №4

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

В итоге получили зашифрованный текст «UMQVMYUST». На рисунке 13 показали зашифровку и расшифровку текста «KISLIAKOV» с помощью ключа «KEY».

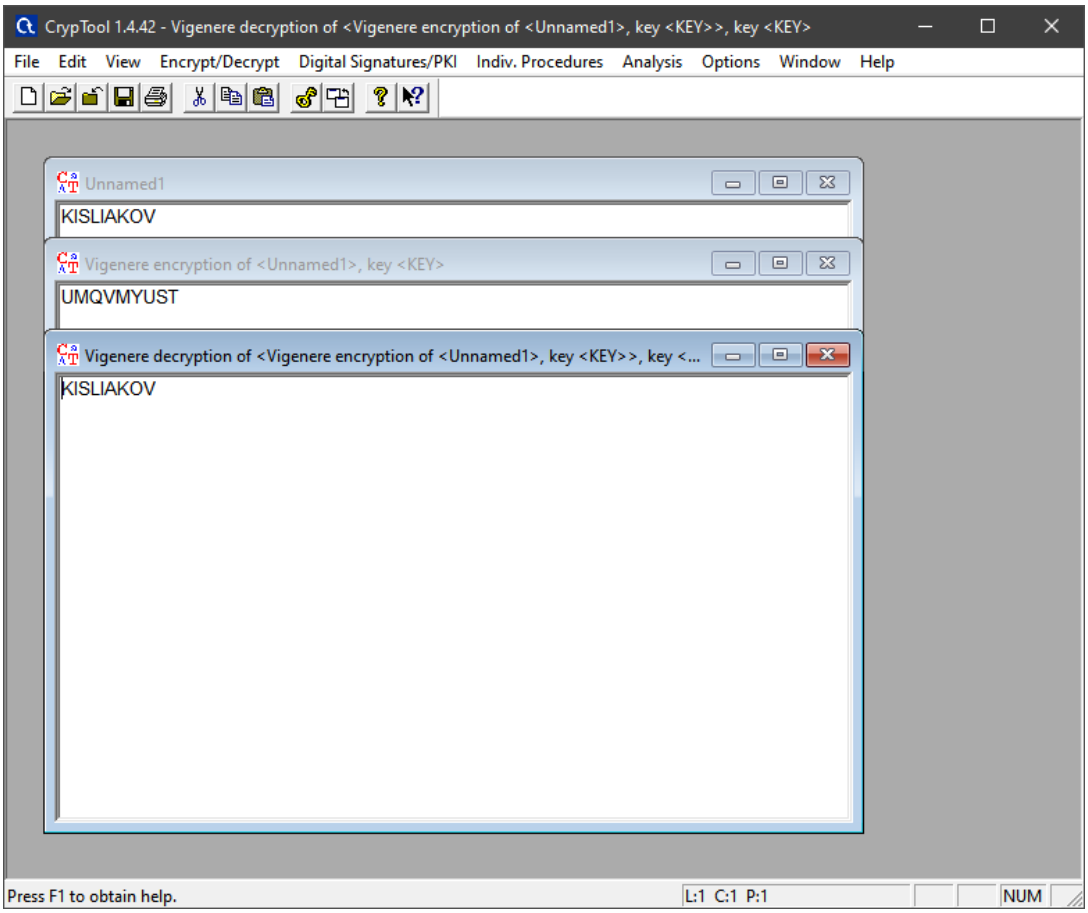

Рисунок 13 – Зашифровка и расшифровка

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

На рисунке 14 произведена атака на шифротекст, но результат неверен, так как текста слишком.

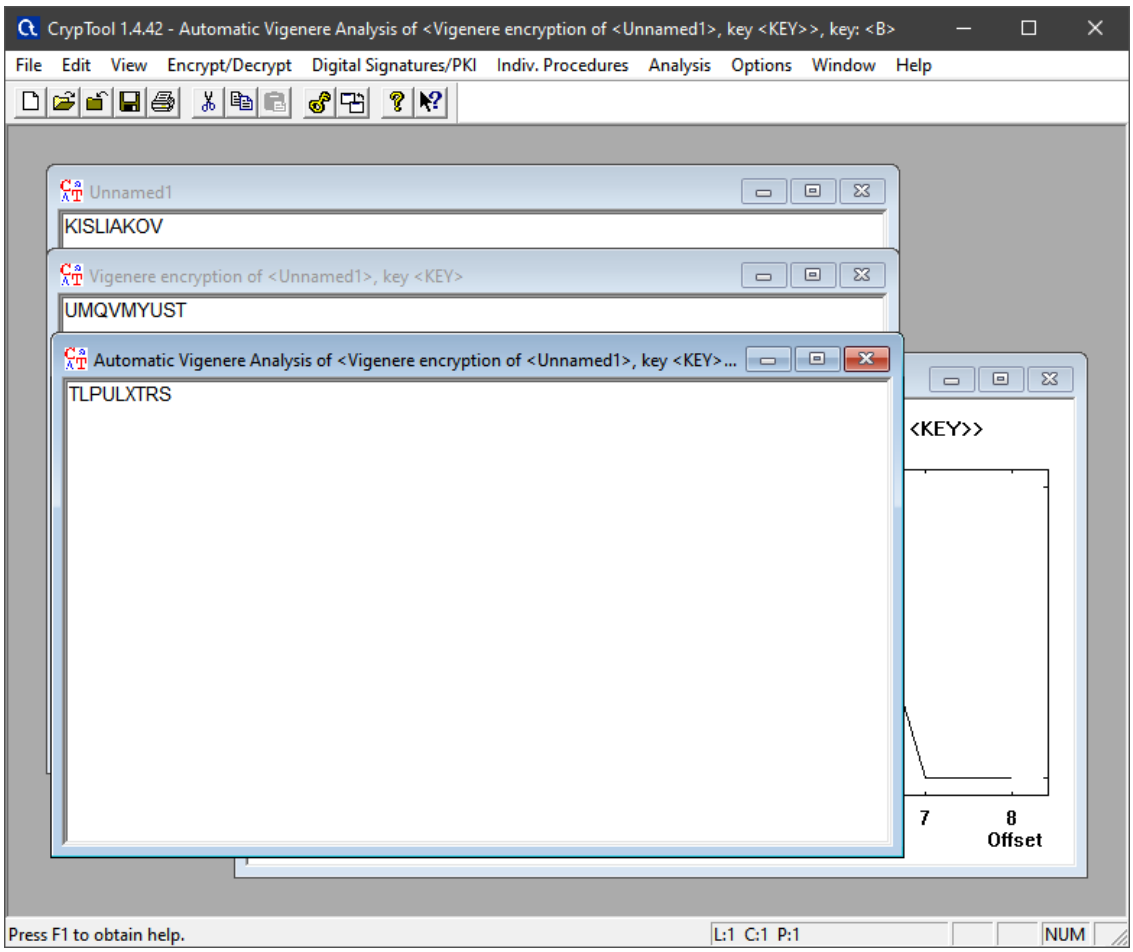

Рисунок 14 – Атака на шифротекст

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

На рисунке 15 провели атаку для фрагмента текста из файла English.txt. Для текста с большим количество символов расшифровка удалась.

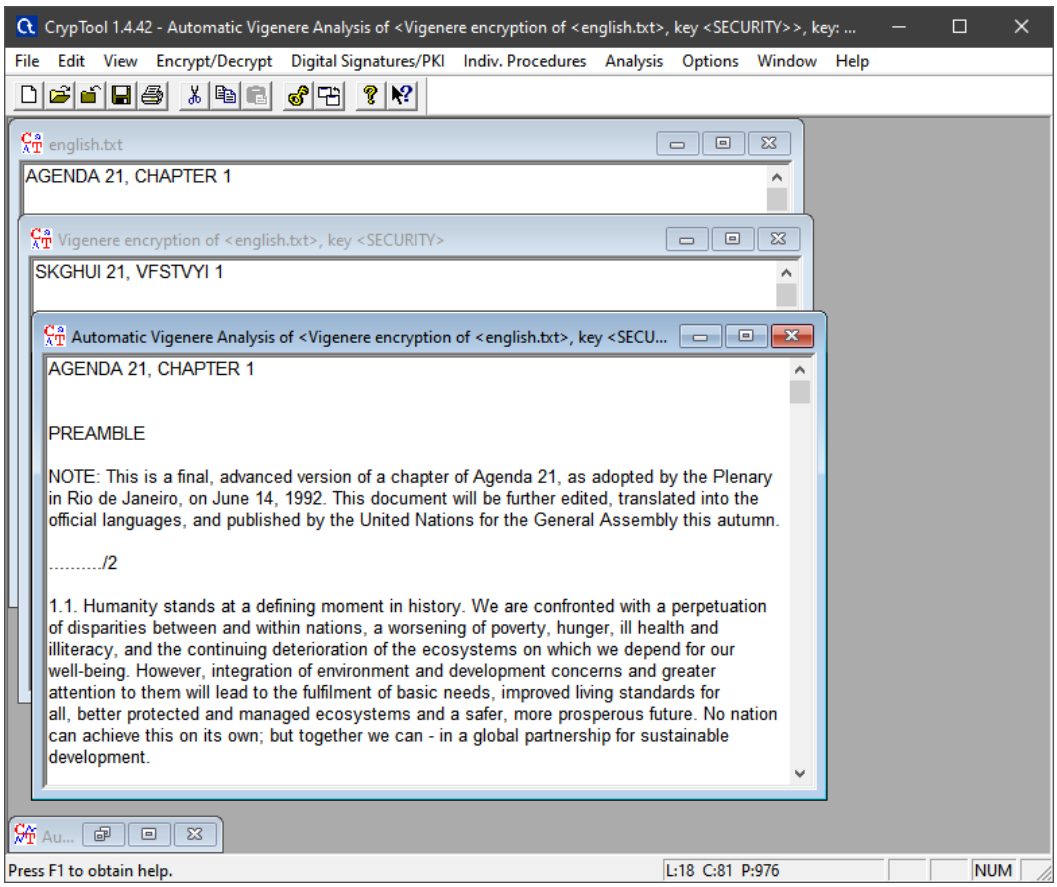

Рисунок 15 – Атака на шифротекст

5. Воспроизвести эту атаку в автоматизированном режиме:

а) определить размер ключа с помощью приложения Analysis –> Tools for Analysis –> Autocorrelation;

На рисунке 16 представлен график. Проанализируем график автокорреляции. На графике показаны количества совпадающих символов для сдвигов t = 1, …, 200. Между offset = 1 и offset = 25 – 3 максимумов, поэтому длина ключа = 8.

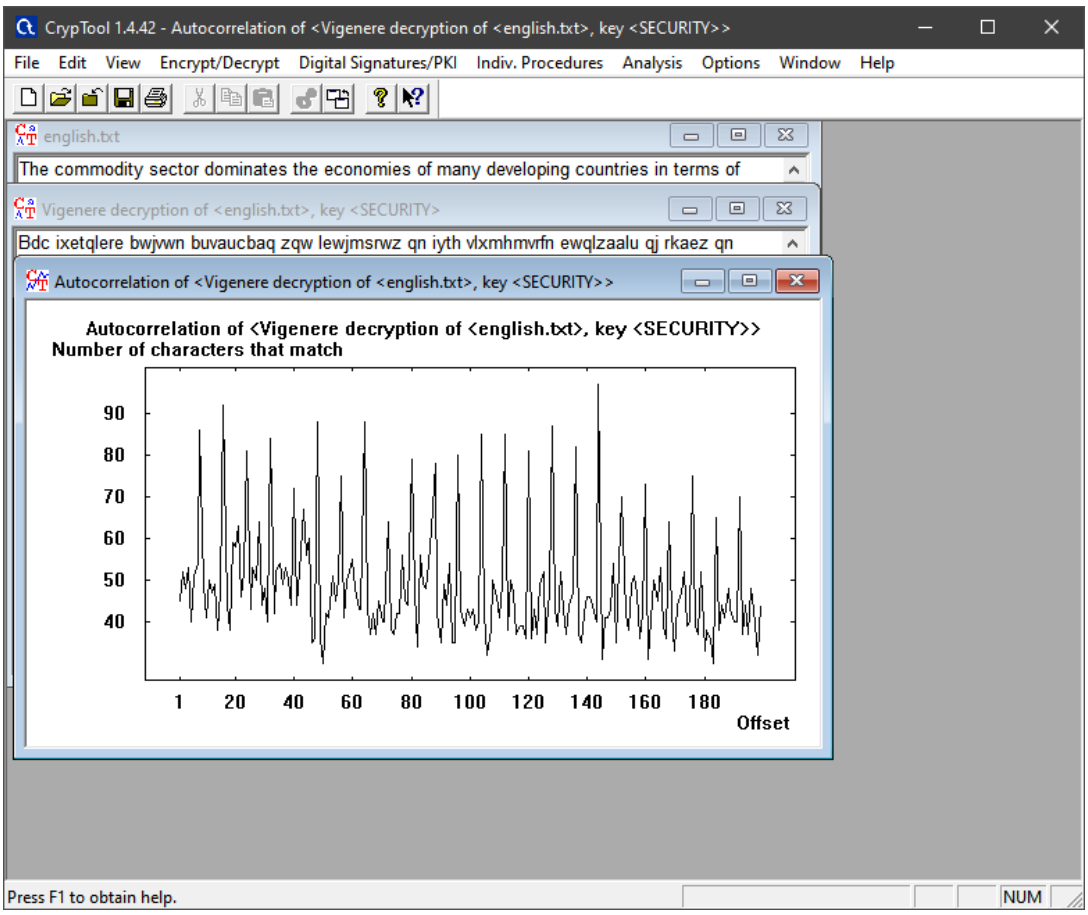

Рисунок 16 – Атака на шифротекст

б) выполнить перестановку текста с размером столбца, равным размеру ключа, приложением Permutation/Transposition;

На рисунке 17 провели перестановку текста с размером столбца, равным размеру ключа, приложением Permutation/Transposition.

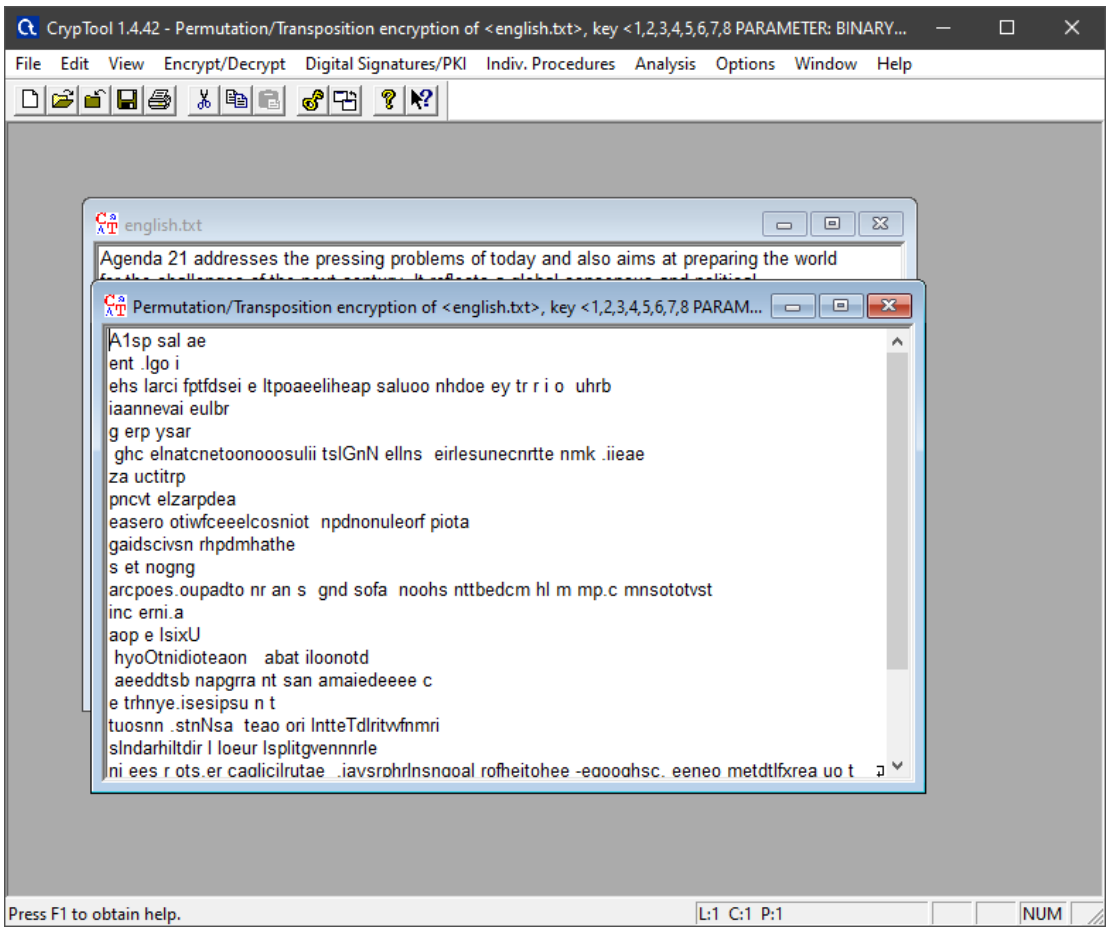

Рисунок 17 – Перестановка текста

в) определить очередную букву ключа приложением Analysis –> Symmetric Encryption(Classic) –> Cipher Text Only –> Caesar.

Далее мы должны разделить текст на количество частей которое равно длине ключа. И для каждой части вычисляется своя буква шифра Цезаря. Получаем отдельно каждую букву ключа. И в итоге получаем полностью весь ключ

6. Выполнить самостоятельную работу: изучить атаку, реализованную в CrypTool 2, опираясь на Help и ссылки на статьи.

Рисунок 18 – CrypTool 2

Шаблон атаки имеет 4 компонентов, основным из которых является Vigenère Analyser. Этот компонент определяет наиболее вероятное ключевое слово, которым был зашифрован текст. Для определения букв ключа компонент использует метод наименьших квадратов. Чтобы вычислить ключ требуется только шифротекст и предположение о языке. В настройках компонента можно указать алфавит шифрования. Vigenère Analyser демонстрирует все рассчитанные ключи. Компонент пытается найти все возможные длины ключа вплоть до 1/40 длины зашифрованного текста.

Наиболее вероятным считается тот ключ, который имеет самый высокий показатель совпадения для всех возможных открытых текстов. Такой ключ подсвечивается серым цветом. Компоненту можно подать на вход длину ключа, тогда будет выбран только один ключ. Чтобы найти наиболее вероятную длину ключа, можно использовать компонент автокорреляции на шифротексте и соединить его с Vigenère Analyser.

2.2 Схема и математические формулы, поясняющие работу шифра.

На рисунке 19 представлена схема шифра «Виженера». Если n – количество букв в алфавите, m_j – номер буквы открытого текста, k_j – номер буквы ключа в алфавите, то шифрование Виженера можно записать следующим образом:

$$c_j = (m_j + k_j)\ mod\ n$$

И расшифрование:

$$m_j = (c_j - k_j) \, mod \, n$$

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

Рисунок 19 – Схема шифра

2.3 Пример работы шифра для выбранных параметров.

На рисунке 20 представлена пример работы шифра.

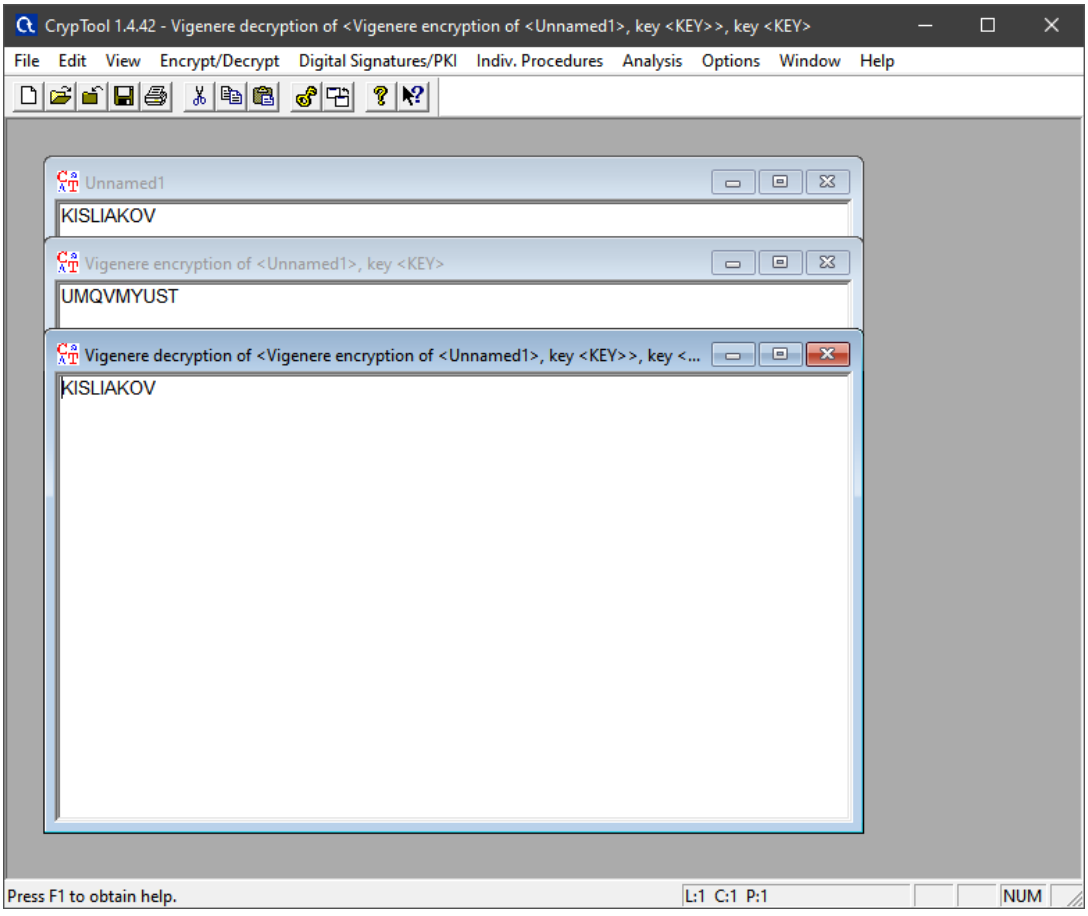

Рисунок 20 – Зашифровка и расшифровка

2.4 Основные характеристики шифра:

а) тип шифра (перестановка, замена, комбинированный);

Тип шифра: замена.

б) ключ шифра;

Ключ шифра: слово.

в) оценка сложности атаки «грубой силы».

Сложность атаки «грубой силы»: $O(\frac{n!}{(n-m)!})$, где n – мощность алфавита, а m – длина ключа

2.5 Описание выполненной процедуры атаки на шифротекст и результат (ключ) этой атаки.

Для расшифровки сообщения требуется знание исходного текста. Далее с помощью Analysis –> Symmetric Encryption(Classic) –> Cipher Text Only –> Vigenere мы атакуем. Чем больше текст, тем лучше.

3. Шифр Хилла (Hill)

3.1 Задание

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

На рисунке 21 нашли шифр Хилла.

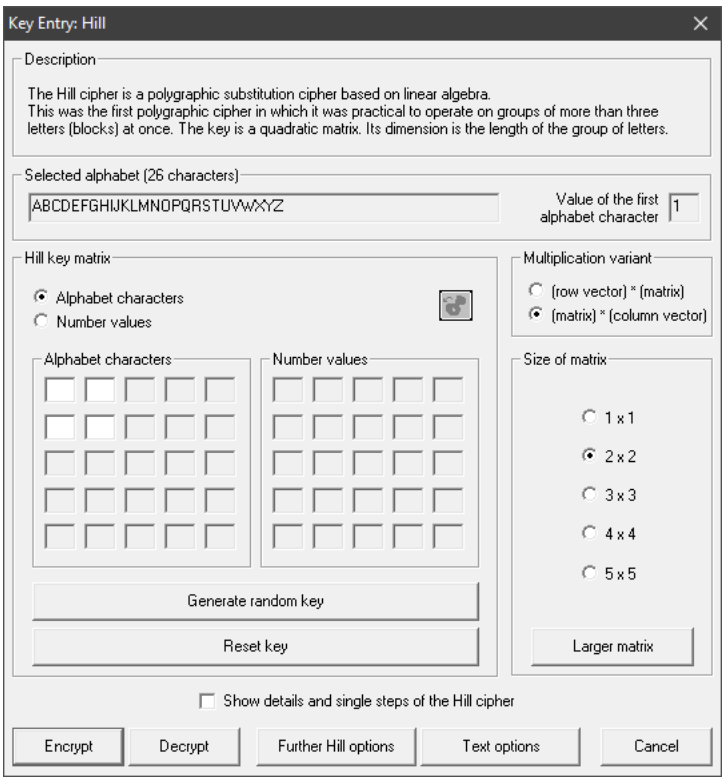

Рисунок 21 – Шифр Хилла

2. Зашифровать и расшифровать текст, содержащий только вашу фамилию (транслитерация латиницей), вручную и с помощью шифра с выбранным ключом 2 × 2. Убедиться в совпадении результатов. Проверить обратимость шифрующей матрицы (ключа).

Зашифруем и расшифруем текст «KISLYKOV»,с помощью ключа {4, 23, 23, 22}, воспользуемся таблицей 5.

Таблица №5

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

$$\begin{pmatrix} 10 & 8 \\ 18 & 11 \\ 24 & 10 \\ 14 & 21 \end{pmatrix} * \begin{pmatrix} 4 & 23 \\ 23 & 22 \end{pmatrix} = \begin{pmatrix} 224 & 406 \\ 325 & 656 \\ 326 & 772 \\ 539 & 784 \end{pmatrix} mod\ 26 = \begin{pmatrix} 16 & 16 \\ 13 & 6 \\ 14 & 18 \\ 19 & 4 \end{pmatrix}$$

Получили следующий зашифрованный текст «QQNGOSTE». На рисунке 22 зашифровали и расшифровали в CrypTool 1, текст «KISLYKOV».

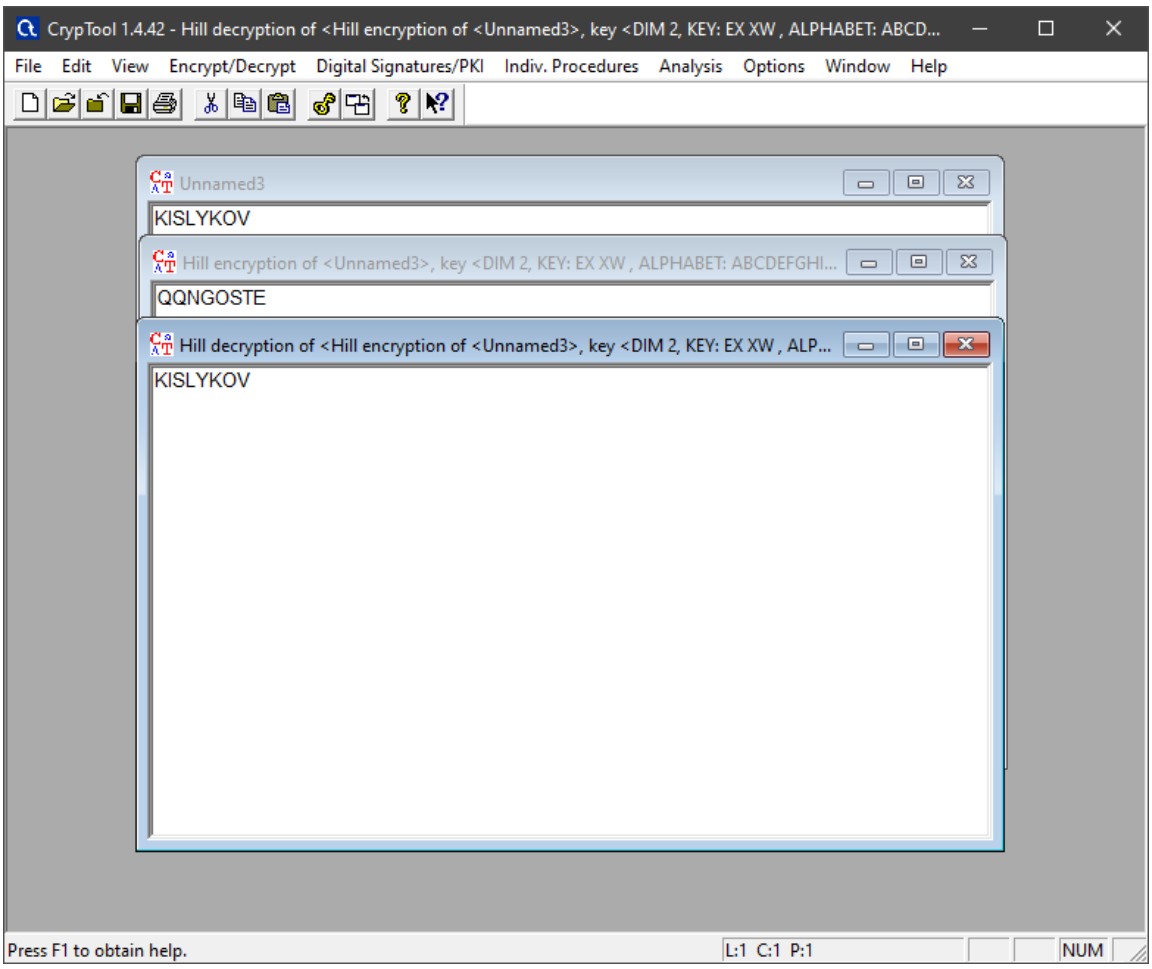

Рисунок 22 – Шифр Хилла

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

Зашифруем текст «DEAR MR KISLYKOV NIKITA ALEXYAVICH THANK YOU VERY MUCH» на рисунке 23. Получили результат на рисунке 24.

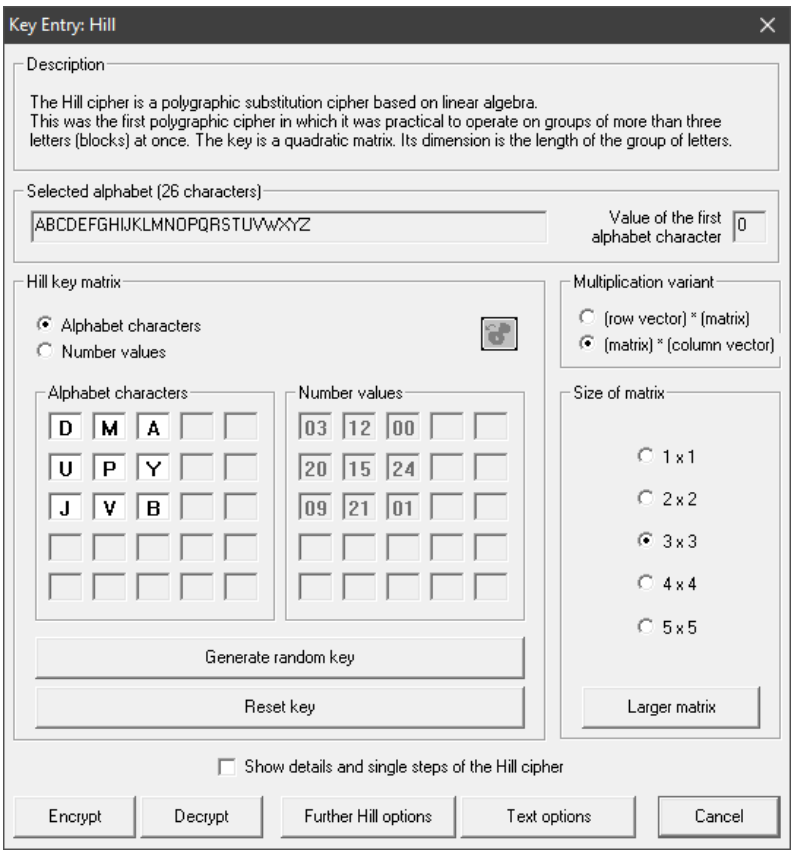

Рисунок 23 – Шифр Хилла

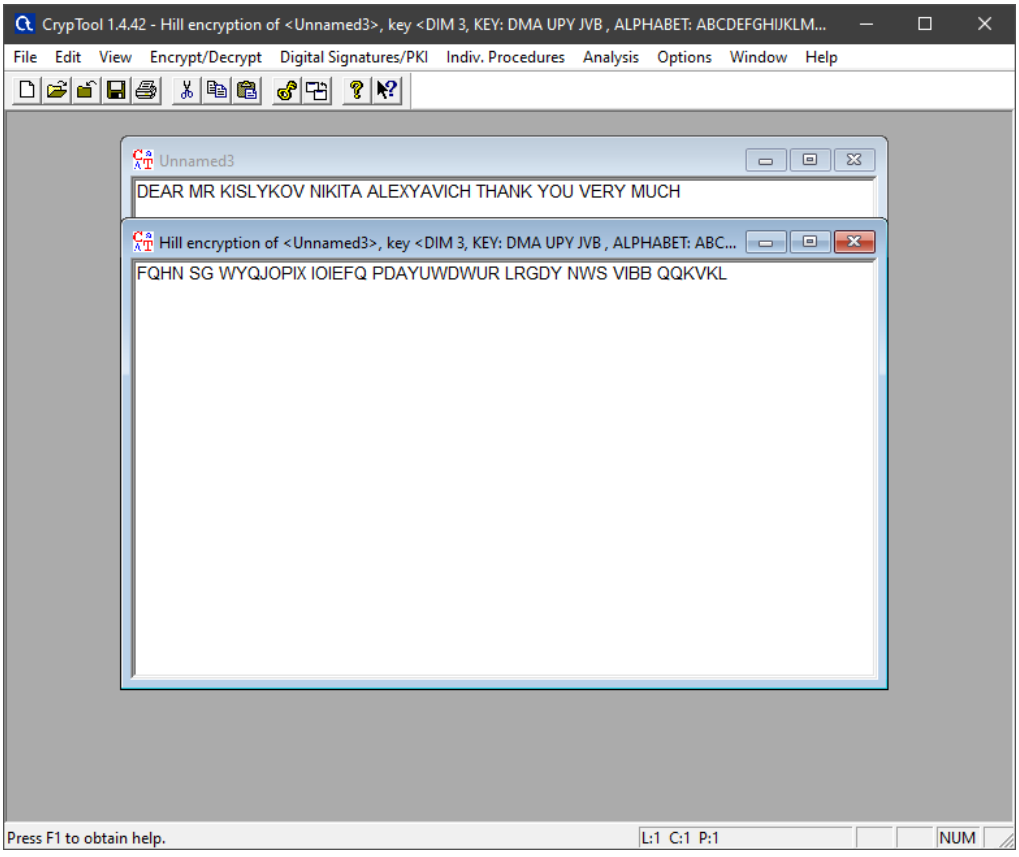

Рисунок 24 – Зашифровка

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

На рисунке 25 нашли выполнили атаку на основе знания открытого ключа.

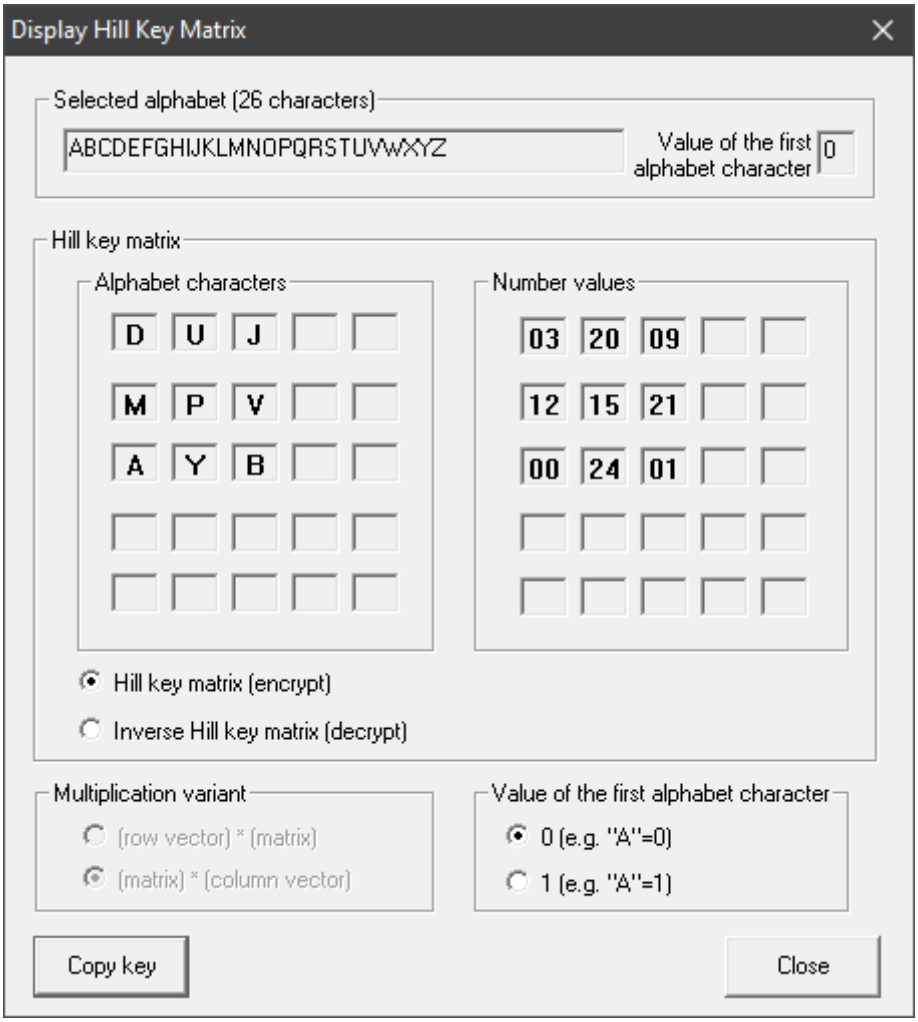

Рисунок 25 – Атака

5. Выполнить самостоятельную работу: обменяться шифровками с коллегой по учебной группе для дешифрования при условии, что формы обращения и завершения сообщения известны. Размерность использованного ключа держать в секрете.

Шифротекст от коллеги: «LYZT VN BBLZF JPQRC IWN PPRC GIGPQ», на рисунке 26 нашли ключ.

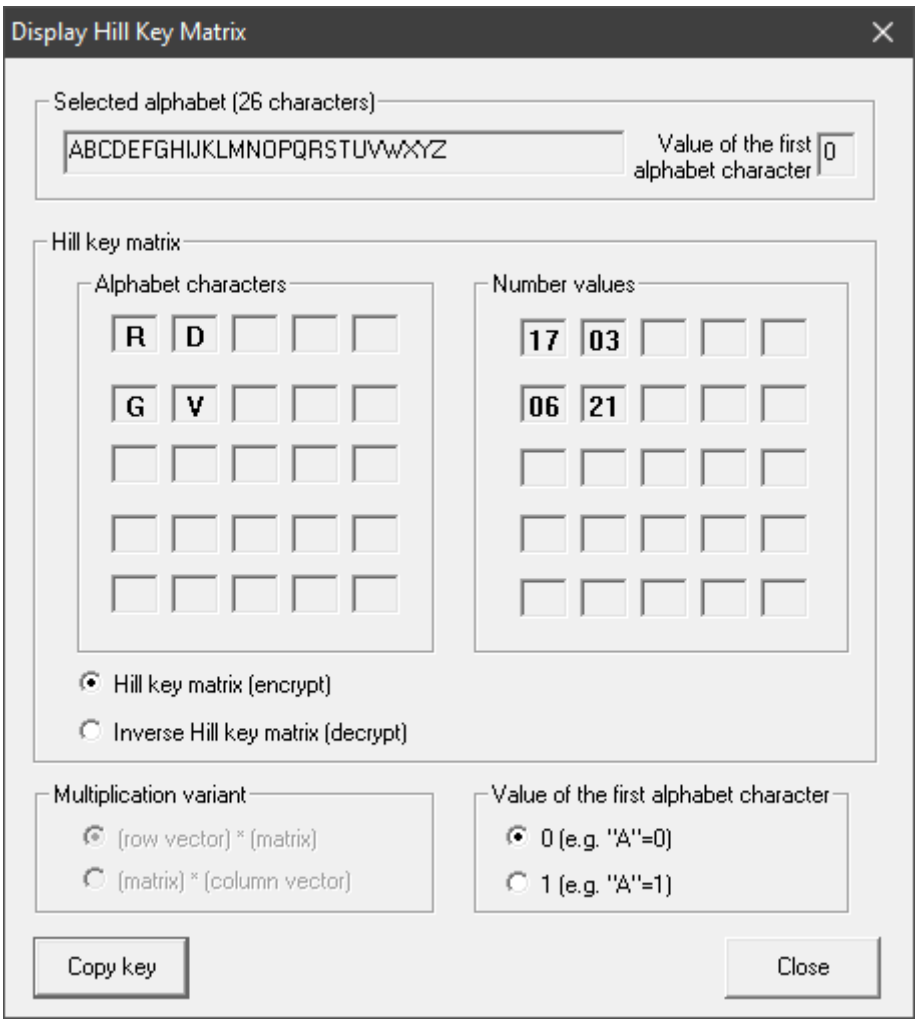

Рисунок 26 – Ключ

3.2 Схема и математические формулы, поясняющие работу шифра. Пример вычисления шифрующей и расшифровывающей матриц

Шифрование: $C = E(K, P) = KP\ (mod\ 26)$

Расшифрование: $P + D(K, C) = K^{-1}C\ (mod\ 26) = K^{-1}KP\ (mod\ 26) = P$

Пример:

Таблица №5

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

$$\begin{pmatrix} 10 & 8 \\ 18 & 11 \\ 24 & 10 \\ 14 & 21 \end{pmatrix} * \begin{pmatrix} 4 & 23 \\ 23 & 22 \end{pmatrix} = \begin{pmatrix} 224 & 406 \\ 325 & 656 \\ 326 & 772 \\ 539 & 784 \end{pmatrix} mod\ 26 = \begin{pmatrix} 16 & 16 \\ 13 & 6 \\ 14 & 18 \\ 19 & 4 \end{pmatrix}$$

На рисунке 27 представлена схема шифра.

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \pmod{26},$$

Рисунок 27 – Схема

3.3 Реализация в CrypTool 1 (скриншот, спецификация параметров)

На рисунке 28 шифр Хилла. В данном шифре нам доступен выбор алфавита а также задать наш ключ в виде матрицы.

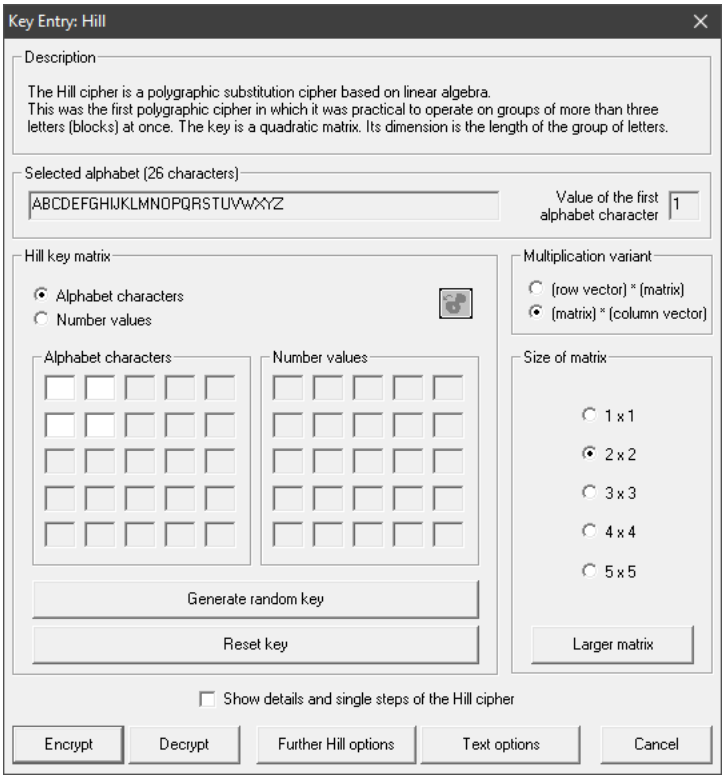

Рисунок 28 – Шифр Хилла

3.4 Пример работы шифра для выбранных параметров и текста сообщения

На рисунке 29 зашифровали и расшифровали в CrypTool 1, текст «KISLYKOV».

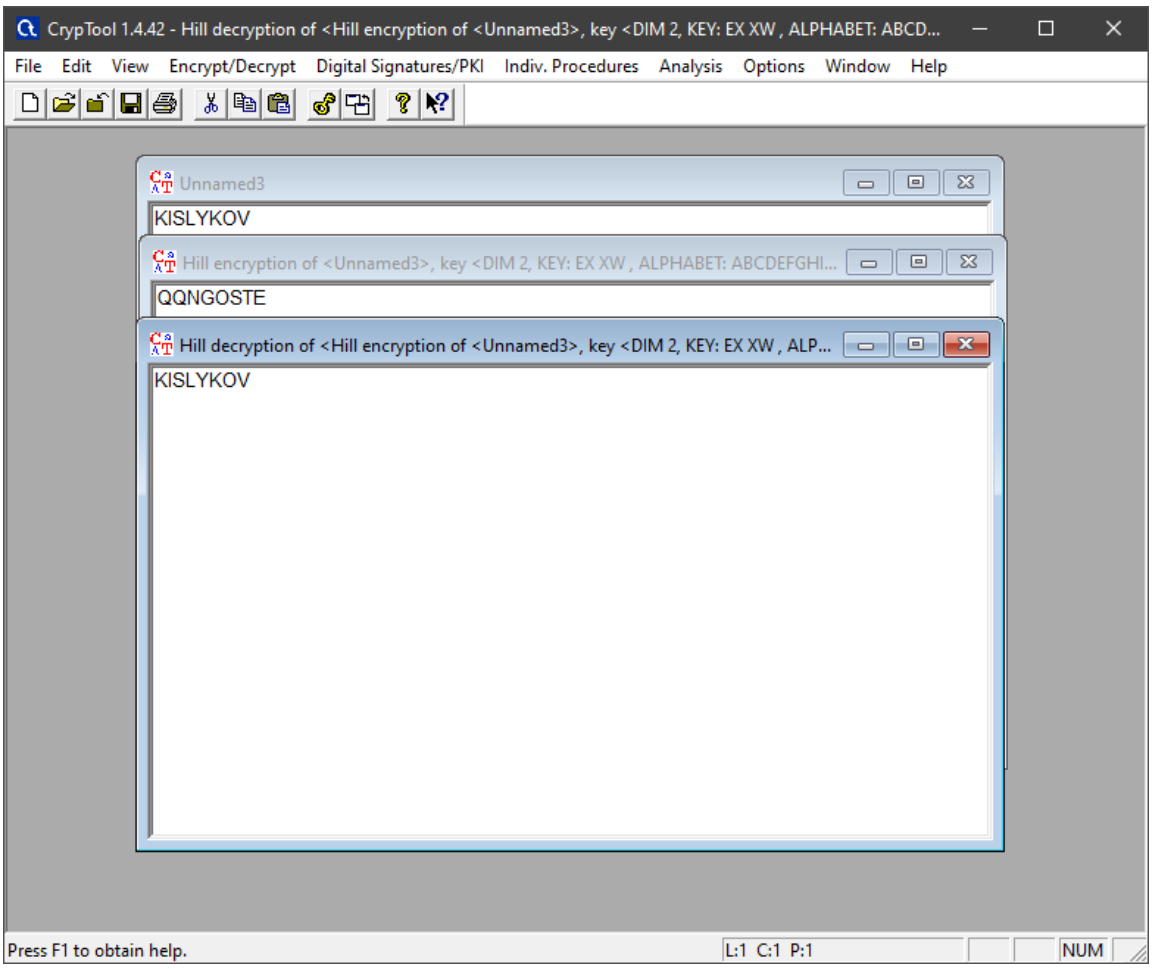

Рисунок 29 – Шифр Хилла

3.5 Основные характеристики шифра:

а) тип шифра (перестановка/замена/комбинированный) и размер блока данных;

Тип шифра: блочный.

б) ключ шифра;

Ключ шифра: шифрующая матрица.

в) оценка сложности атаки «грубой силы».

Сложность атаки «грубой силы»: $O(n^{mxm})$, где n – мощность алфавита, а m – размер блока текста, подлежащего шифрованию.

3.6 Описание атаки на шифр с использованием утилит Cryp Tool 1

Зная исходный и зашифрованный текст, можно с помощью Analysis –> Symmetric Encryption(classic) –> Known Plaintext найти ключ, то есть матрицу.

Вывод

1. Шифр «Сцитала» (Scytale)

Шифр Scytale – шифр перестановки, зависящий от количества строк и размера смещения.

В ходе выполнения работы несколько раз было выполнено шифрование и расшифровка текста. А также, была выполнена модификация шаблона атаки «грубой силы», которая заключается в переборе параметров, от которых зависит перестановка, в приложении CrypTool 2, исходный текст был сначала зашифрован, а далее с помощью атаки «грубой силы» - расшифрован. В результате чего, были получены практические навыки работы с данным шифром.

Тип шифра: перестановка.

Ключ шифра: количество рёбер и размер смещения.

Сложность атаки «грубой силы»: $O(n^2)$.

2. Шифр Виженера (Vigenere)

В ходе выполнения работы по шифру Vigenere было выполнено шифрование и расшифровка различного текста. А также, были выполнены атаки на шифротекст различной длины с помощью приложений CrypTool1 и CrypTool2, выяснено, что атака будет эффективна для текста большой длинны. В результате, были получены практические навыки работы с данным шифром

Тип шифра: замена.

Ключ шифра: слово.

Сложность атаки «грубой силы»: $O(\frac{n!}{(n-m)!})$, где n – мощность алфавита, а m – длина ключа.

3. Шифр Хилла (Hill)

В ходе выполнения работ по шифру Hill было выполнено шифрование и расшифровка текста. Были успешно выполнены атаки на основе знания открытого текста на шифротекст различной длины с помощью приложения

CrypTool1. В результате, были получены практические навыки работы с данным шифром.

Тип шифра: блочный.

Ключ шифра: шифрующая матрица.

Сложность атаки «грубой силы»: $O(n^{mxm})$, где n – мощность алфавита, а m – размер блока текста, подлежащего шифрованию.