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

ОТЧЕТ

по лабораторной работе №1-2-3
по дисциплине «Криптография и защита информации»
Тема: Распознавание цифр

Студент гр. 8383 _____ Дейнега В. Е.

Преподаватель _____ Племянников А.К.

Санкт-Петербург
2021

В – 2.

Цель работы

Исследовать работу трех классических шифров согласно варианту, а именно шифры “Цезаря”, “Двойной перестановки” и “Плейфеера”.

Шифр “Цезаря”.

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.

Выполнение работы

1) Зашифруем и расшифруем текст, содержащий фамилию латиницей, рис. 1.

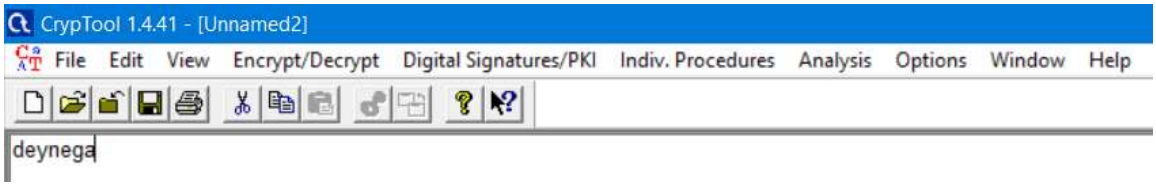

Рисунок 1 – Шифротекст.

Выставим параметры шифра, рис. 2.

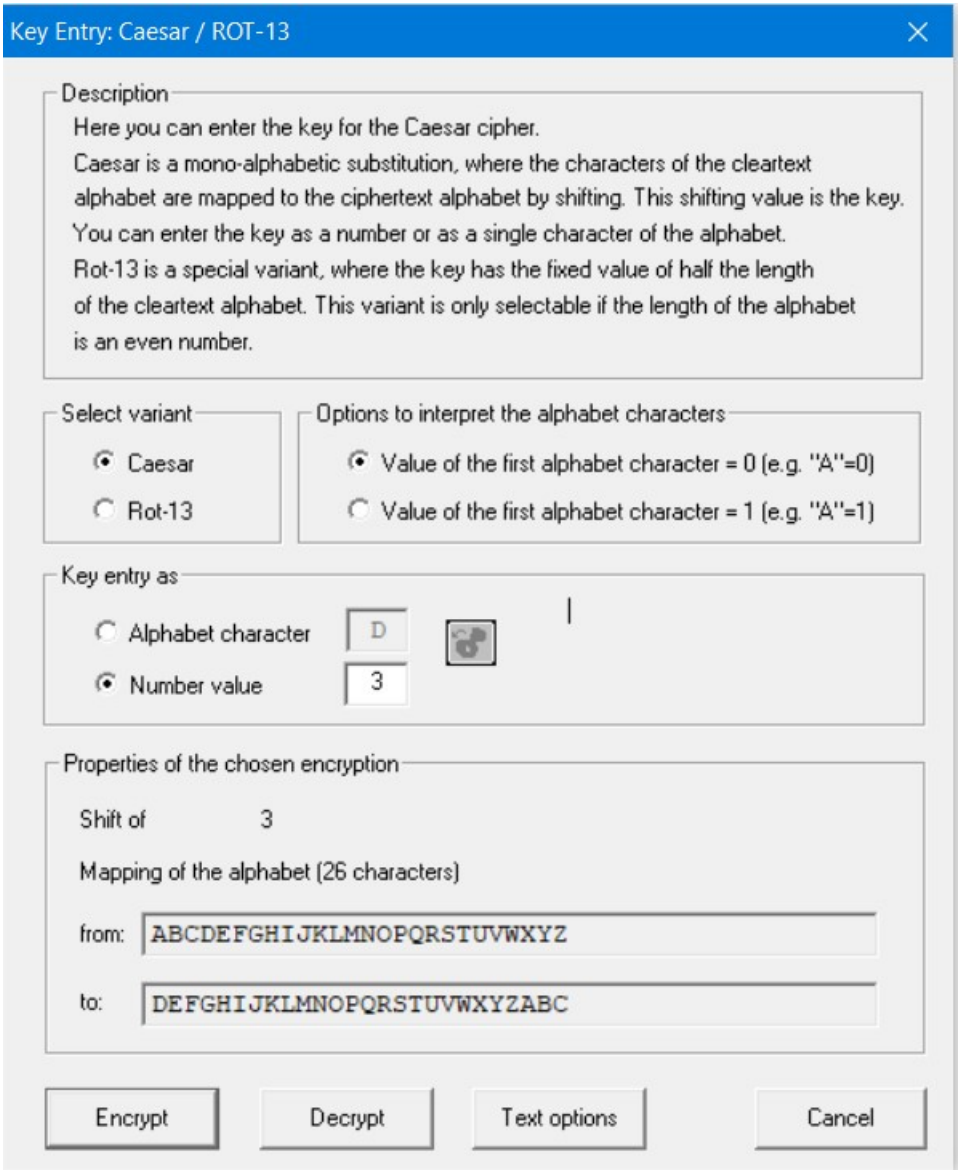

Рисунок 2 – Парметры шифра Цезаря.

Результат представлен на рис. 3.

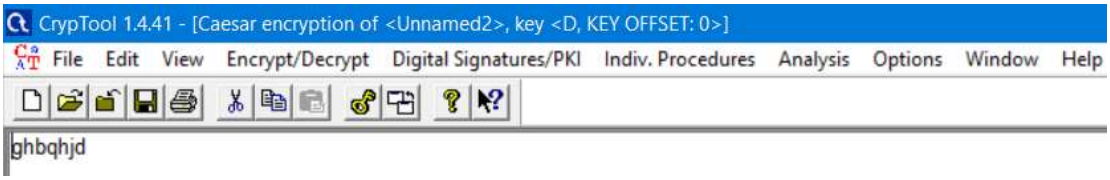

Рисунок 3 – Результат работы шифра Цезаря.

На таблице 1 приведена схема того как преобразуются символы согласно шифру цезаря с ключом 3.

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
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

Таблица 1

Расшифруем полученный текст вручную.

g -> **d**, h -> **e**, b -> **y**, q -> **n**, h -> **e**, j -> **g**, d -> **a**.

А также с помощью программы, рис. 4

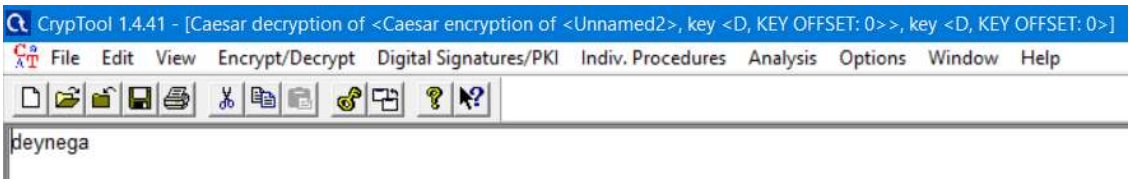

Рисунок 4 – Расшифрованный текст.

Результаты совпали.

2) Проведем атаку на данный шифр.

Для начала зашифруем текст средней длинны из файла CrypTool-en.txt, используя ключ 3 (C), результаты шифровки приведены на рис. 5.

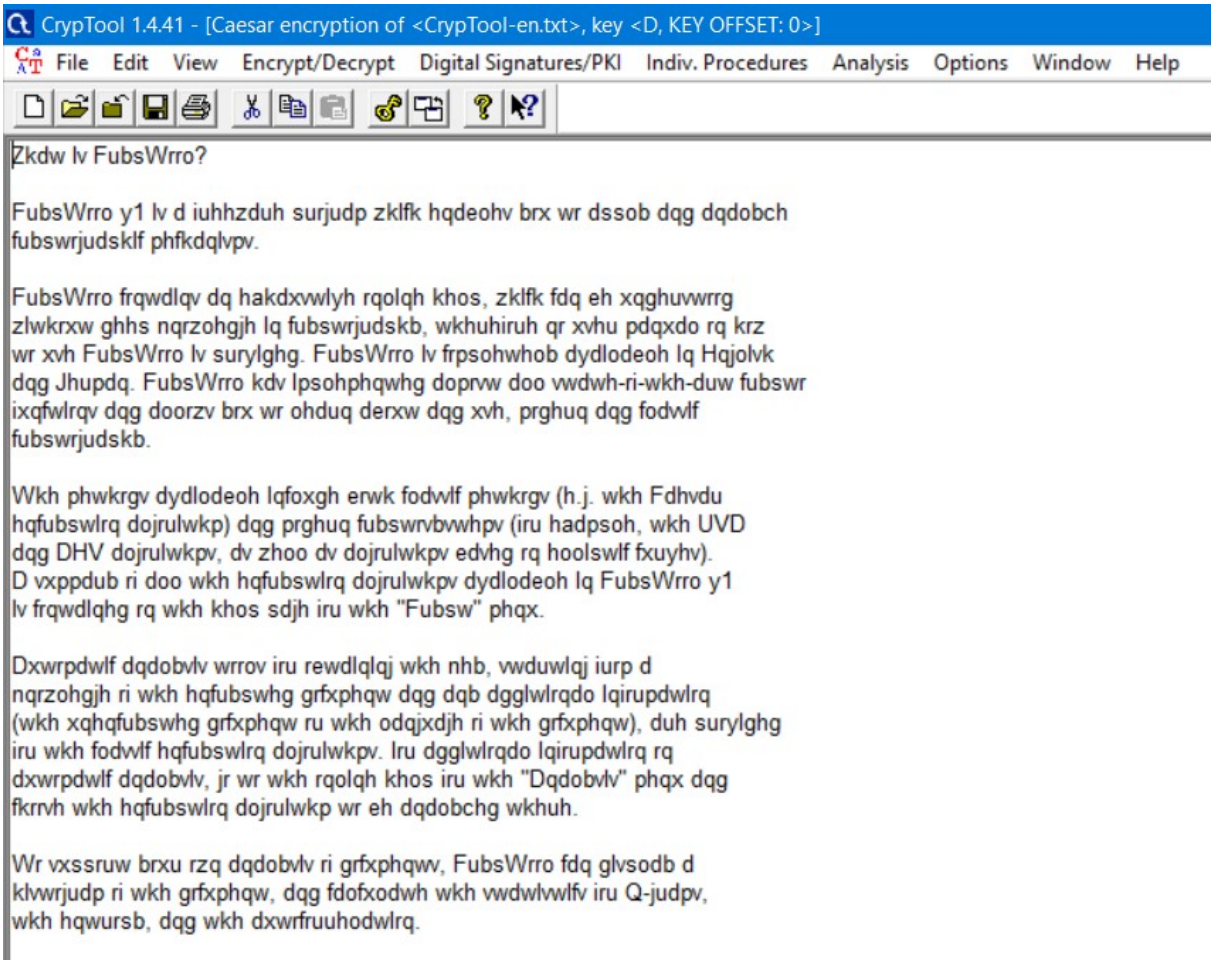

Рисунок 5 – Зашифрованный текст.

Построим гистограмму частот букв английского языка по эталонному файлу English.txt, а также по зашифрованному тексту, рис. 6, 7.

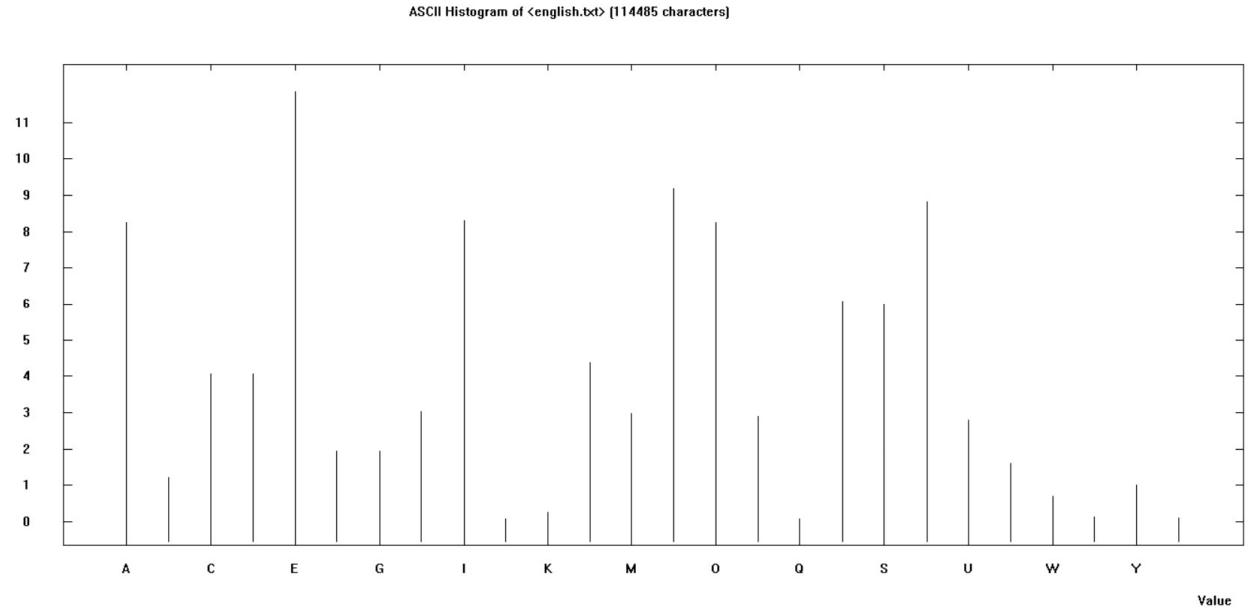

Рисунок 6 – Гистограмма частот букв английского языка по эталонному файлу English.txt.

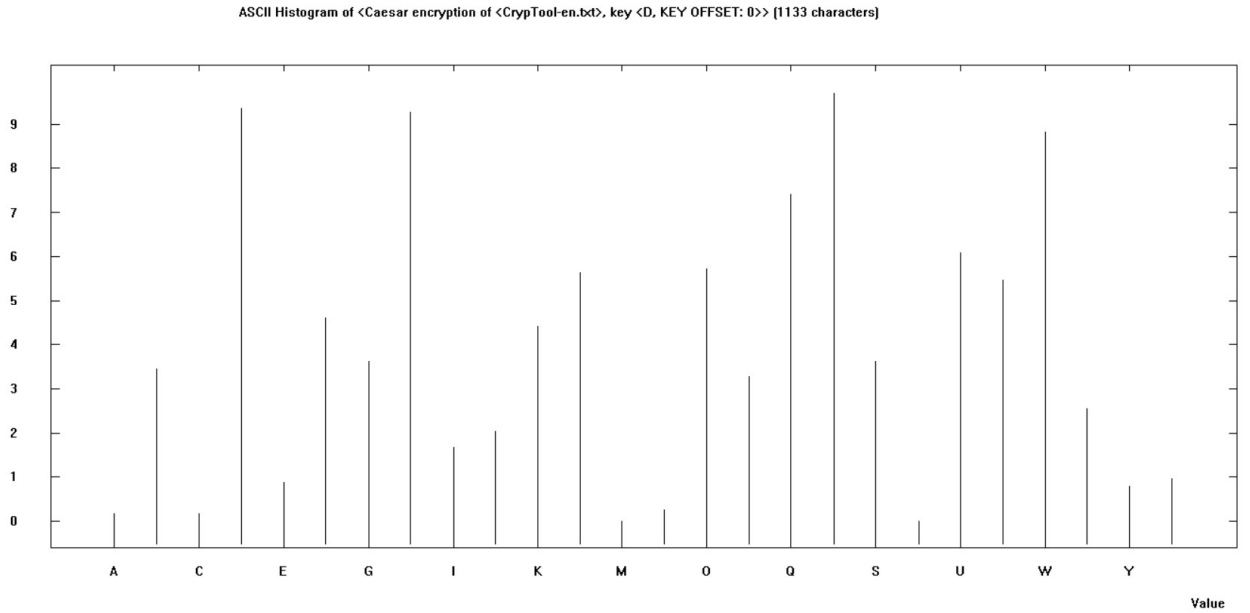

Рисунок 7 - Гистограмма частот букв английского языка по зашифрованному тексту.

Можно заметить, что паттерн на рис. 7 совпадает с паттерном на рисунке 6, если сместить график на рис. 7 на 3 пункта влево. Из этого можно сделать вывод, что ключ шифра равен 3 (C). Тип шифра цезаря – замена.

3) Атака грубой силой на шифр Цезаря заключается в переборе всех сдвигов, например, в английском языке их будет 25, исходя из этого можно считать, что сложность атаки грубой силой на шифр Цезаря $O(n)$, где n – количество всех возможных сдвигов.

Шифр двойной перестановки(Permutation/Transposition)

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 с 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 message THANKS», используя только одинарную перестановку.

6. Передать шифровку коллеге по учебной группе, для дешифровки при условии, что формы обращения и завершения письма известны.

7. Самостоятельно изучить атаку, реализованную в CrypTool 2, опираясь на Help и ссылки на статьи.

Выполнение работы

1) Зашифруем следующий текст “deynegaviktorevgenievih” с помощью утилиты criptools и вручную, установим параметры как на рис. 8.

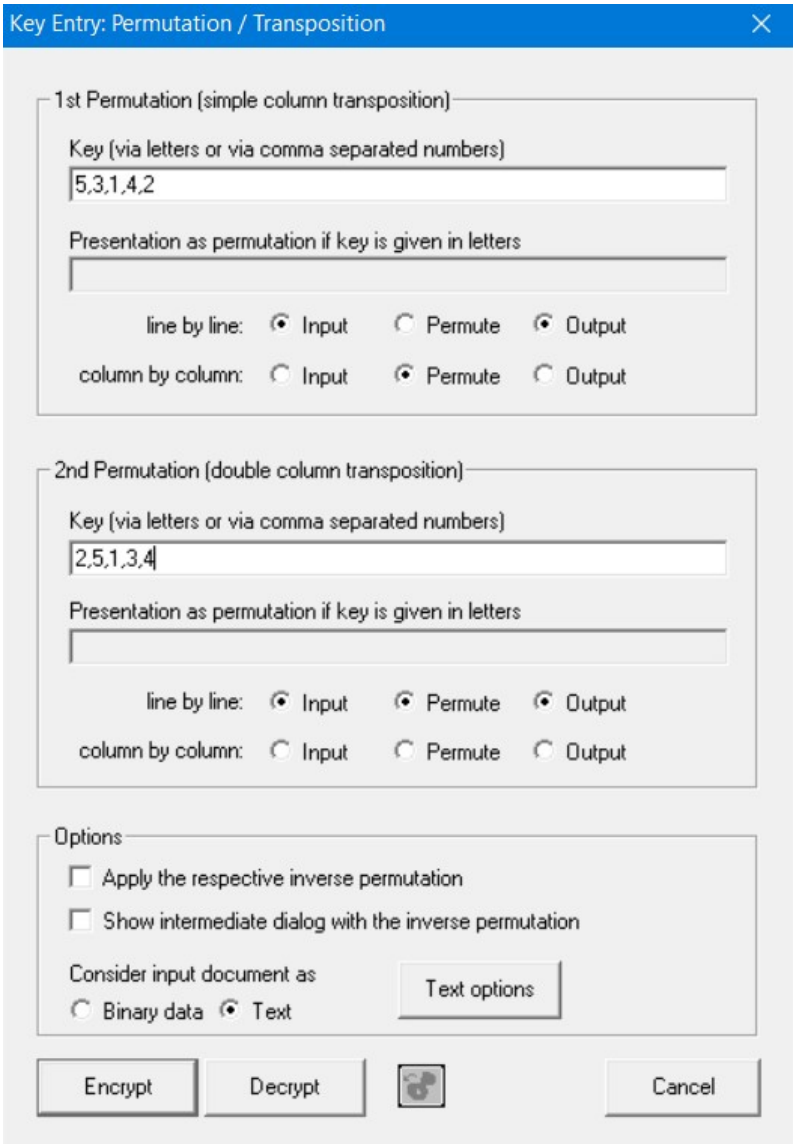

Рисунок 8 – Параметры шифра.

Зашифрованный текст: “rvoetyeendneeighivvkaig”. Для проверки зашифруем текст руками.

	5	3	1	4	2
2	d	e	y	n	e
5	g	a	v	i	k
1	t	o	r	e	v
3	g	e	n	i	e
4	v	i	h		

	1	2	3	4	5
2	y	e	e	n	d
5	v	k	a	i	g
1	r	v	o	e	t
3	n	e	e	i	g
4	h		i		v

	1	2	3	4	5
1	r	v	o	e	t
2	y	e	e	n	d
3	n	e	e	i	g
4	h		i		v
5	v	k	a	i	g

Текст был зашифрован правильно. Расшифровав полученный текст с теми же параметрами, получим исходную строку. При шифровке утилита предлагает выбрать несколько параметров, рис. 9.

Рисунок 9 – Различные параметры шифра.

Input/output line by line значит, что информация в матрицу будет заносится/читаться по строкам. Permute line/column by line/column определяет будет программа работать с информацией как со строкой или как со столбцом.

Данный шифр является шифром-перестановкой. Ключом данного шифра является набор чисел, который мы в последствии переставляем в нужном порядке. Сложность атаки грубой силы составляет $O(n!*m!)$, где m и n – количество строк и столбцов, факториал берется из того факта, что количество перестановок из n чисел равно $n!$.

2) Проведем атаку на этот шифр с помощью инструментов CrypTool 1.0. Для этого зашифурем текст только с помощью изменений в колонке, ключ – 3, 1, 2. Зашифрованный текст: eydegnviatokevrengevihi. Теперь проведем атаку, зная исходный текст, рис. 10.

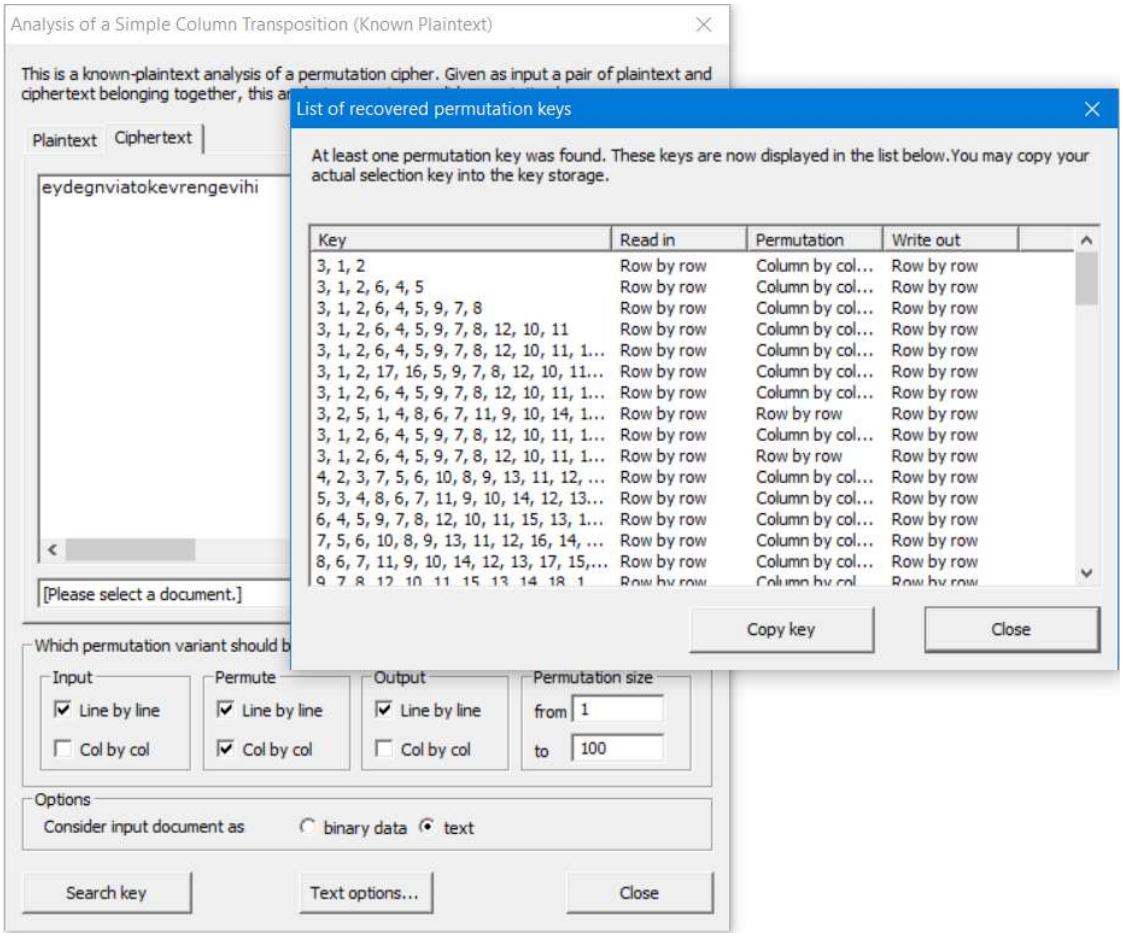

Рисунок 10 – Атака CrypTool 1.0.

В ходе этой атаки программа для каждого числа от 1 до 100 генериует все перестановки и проверяет, получается ли исходный текст из шифра, если получается – ключ найден.

3) Проведем атаку на шифр в CrypTool 2.0. CrypTool 2.0. предлагает несколько атак на шифр, воспользуемся методом восхождения к вершине. Метод работает следующим образом. Изначально ключ инициализируется случайным образом, далее запускается цикл, который действиует до тех пор, пока сосед ключа может дать лучший результат при дешифровке изначального текста. Результат атаки предствален на рис. 13

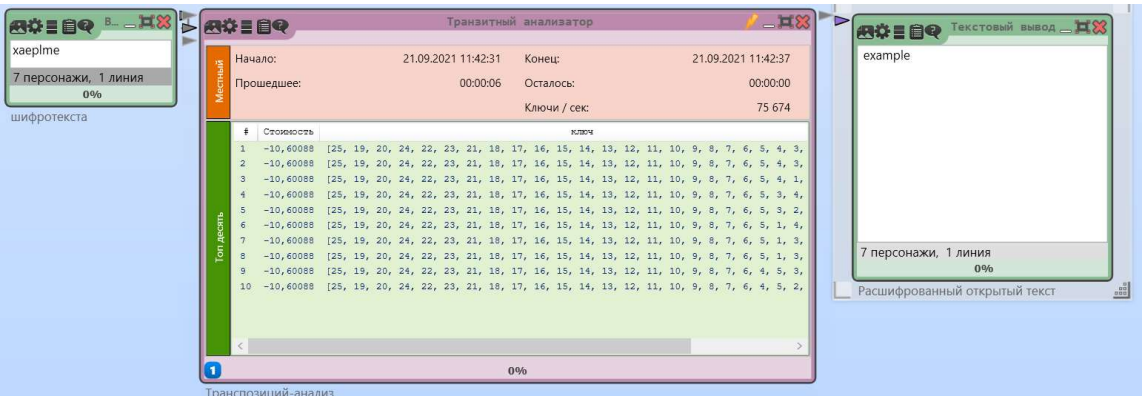

Рисунок 13 – Hill climbing.

Шифр Плейфера (Playfair)

Задание.

1. Найти шифр в CrypTool 1.0.: Encrypt/Decrypt-> Symmetric(Classic).

2. Зашифровать и расшифровать текст содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра с выбранной ключевой матрицей. Убедиться в совпадении результатов.

3. Зашифровать текст с произвольным сообщением в формате «DEAR ALL THANK YOU FOR ПРОИЗВОЛЬНЫЙ ТЕКСТ», используя выбранную шифрующую матрицу.

4. Выполнить атаку на основе знания части открытого текста, используя приложение из Analysis-> Symmetric Encryption(classic)->Manual Analysis. В качестве известного фрагмента текста использовать «DEAR ALL THANK YOU FOR»: a. Познакомьтесь с методикой проведения атаки в разделе Work through the examples из Help b. Познакомьтесь со спецификацией приложения для проведения атаки в разделе Analysis-> Symmetric Encryption(classic)- >Manual Analysis->Playfair

5. Передать произвольную шифровку коллеги по группе для расшифрования при условии, что форма обращения, используемая в сообщении, известна. Размер использованной матрицы (ключа) держать в секрете.

Выполнение работы

1) Чтобы зашифровать текст его необходимо разбить на пары символов. Процесс шифрования подчиняется следующим правилам:

   1. Если два символа совпадают или остался один символ, то к первому символу добавляется X и шифруется уже эта пара.

   2. Если символы находятся в одной строке, то они замещаются на расположенные в ближайших от них справа символы.

   3. Если символы в одном столбце, то они замещаются на расположенные ниже в ближайших от них клетках

   4. Если символы находятся в разных углах образуемого ими прямоугольника, то они заменяются на символы, стоящие в противоположных углах этого прямоугольника, в тех же строках. Расшифровка сообщения происходит инверсией данных правил.

2) Зашифруем текст “deynega” с помощью CrypTool 1.0., рис. 11.

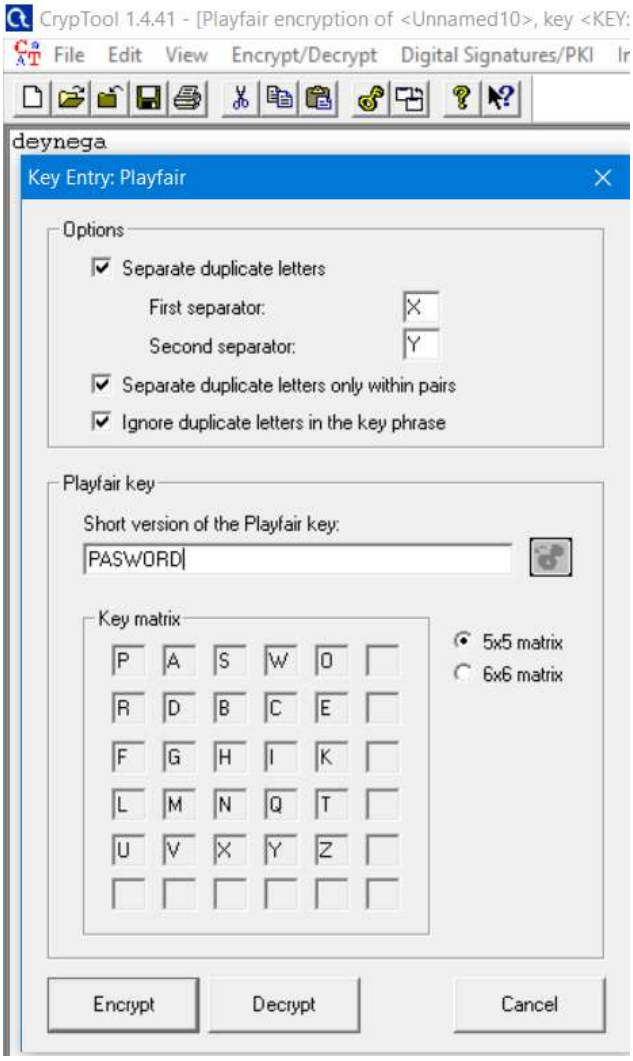

Рисунок 11 – Параметры шрифа Плейфеера.

Получим шифротекст “RC XQ DK SV”, который сопадает с текстом, который получился в результате ручного шифрования.

Данный шифр является шифром-заменой, однако его не так просто анализировать, как другие шифры с заменами из-за того что шифруются не отдельные символы, а биграммы. Также данный шифр является блочным т.к. использует один ключ для шифрования всего текста. Ключом шифра является матрица 5x5, однако в некотрых вариациях матрица формируется на основе секретного слова, которое в данном случае и будет ключом.

Для атаки грубой силой придется рассмотреть 25! вариаций матрицы-ключа.

2) Проведем атаку на шифр с помощью CrypTool 1.0. Зашифруем сообщение “dear all thank you for your help”, рис. 12.

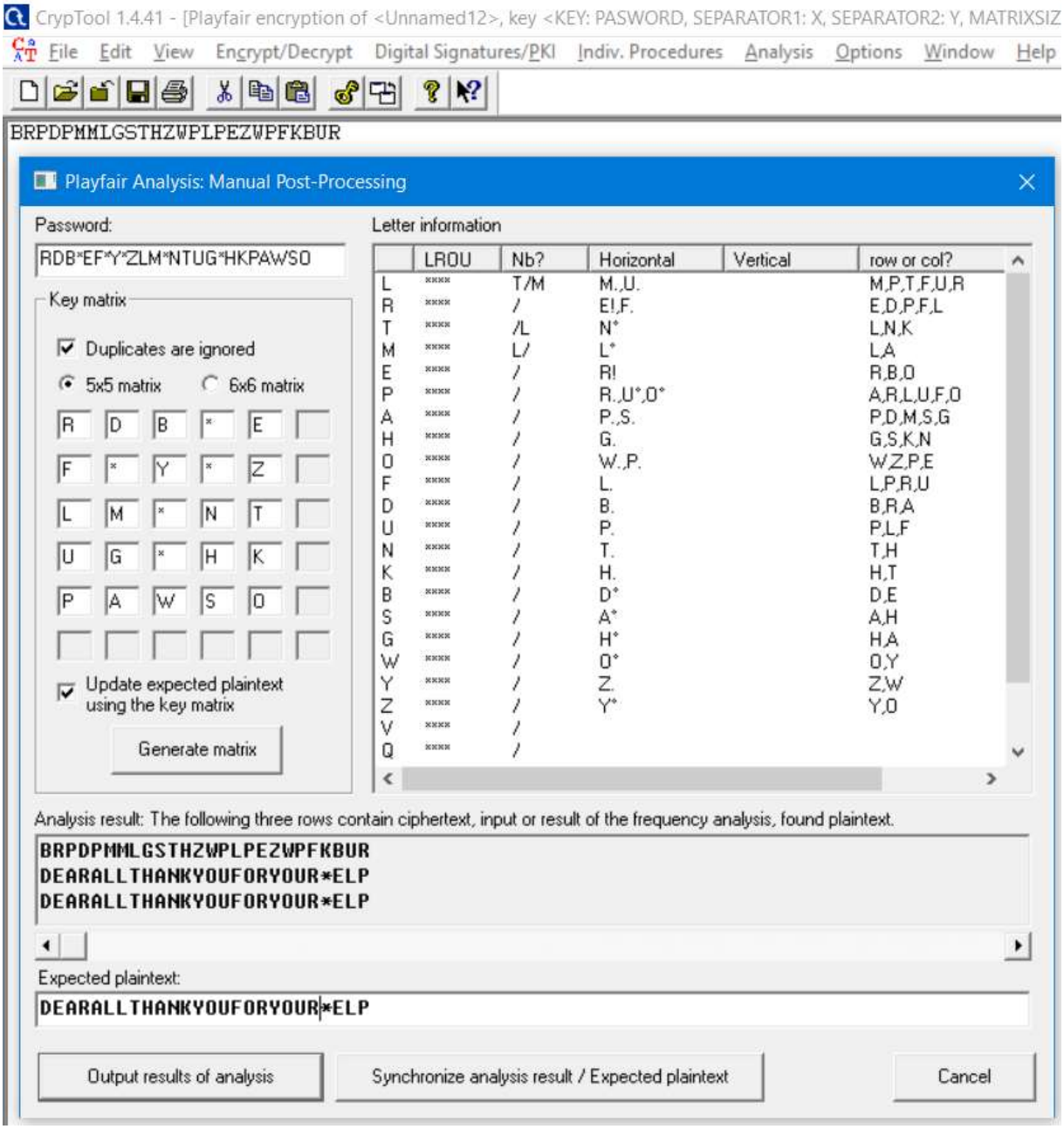

Рисунок 12 – Атака на Playfair.

Атака использует известные фрагменты текста и на их основе предполагает расположение символов в матрице-ключе. В нашем случае слово help явно угадывается, однако ключ не является полным и тем более верным, на более больших фрагментах текста это заметно лучше.

Выводы.

В ходе выполнения лабораторной работы был изучен шифр Цезаря, вручную и с помощью утилиты CrypTool 1.0 был зашифрован и расшифрован текст, результаты совпали. На шифр была проведена атака с помощью частнотного анализа, ключ шифра был успешно найден, при достаточной длине текста шифр крайне уязвим к подобной атаке.

В процеесе выполнения лабораторной работы также использовался шифр двойной перестановки, с его помошью был зашифрован и расшифрован текст. Были изучены параметры шифра в утилите CrypTool 1.0, было выяснено, что алгоритм шифровки может варьироваться. Данный шифр является шифром перестановкой, а сложность взлома грубой силой составляет $O(n!*m!)$. На шифр также была проведена атака с помощью CrypTool 1.0 и CrypTool 2.0, в обоих вариантах ключи получились избыточными, однако верно расшифровывали текст за небольшое время, что говорит о небольшой устойчивости шифра.

Кроме этого был рассмотрен шифр Плейфеера, с его помощью был расшифрован и зашифрован текст, было выяснено, что шифр является блочным шифром-заменой. С помощью CrypTool 1.0 на данный шифр была проведена атака, которую сложно назвать успешной, несмотря на то что человек может угадать зашифрованый текст, ключ, подобранный утилитой неточен и для более больших текстов расшифровку понять крайне сложно.