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

# ОТЧЕТ

**по лабораторной работе №1**

**по дисциплине «Криптография и защита информации»**

**Тема: Изучение классических шифров Scytale, Vigenere, Hill**

Студент гр. 9381 _____ Колованов Р.А.

Преподаватель _____ Племянников А.К.

Санкт-Петербург

2022

**Цель работы.**

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

**Ход работы.**

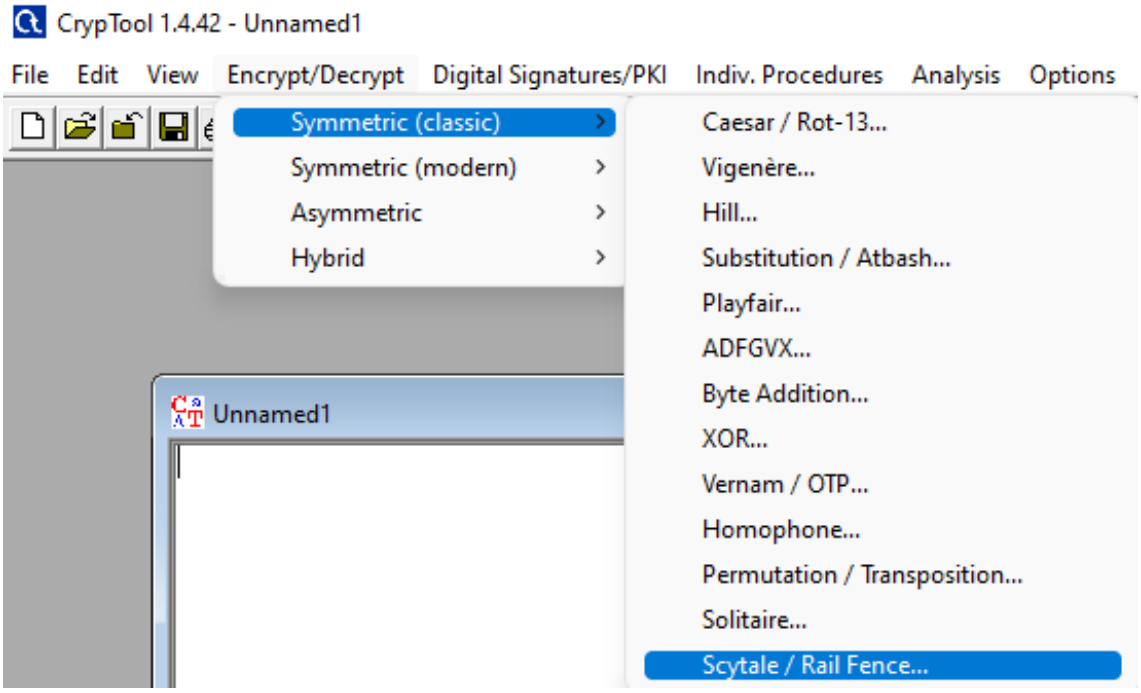
***Шифр Scytale.***

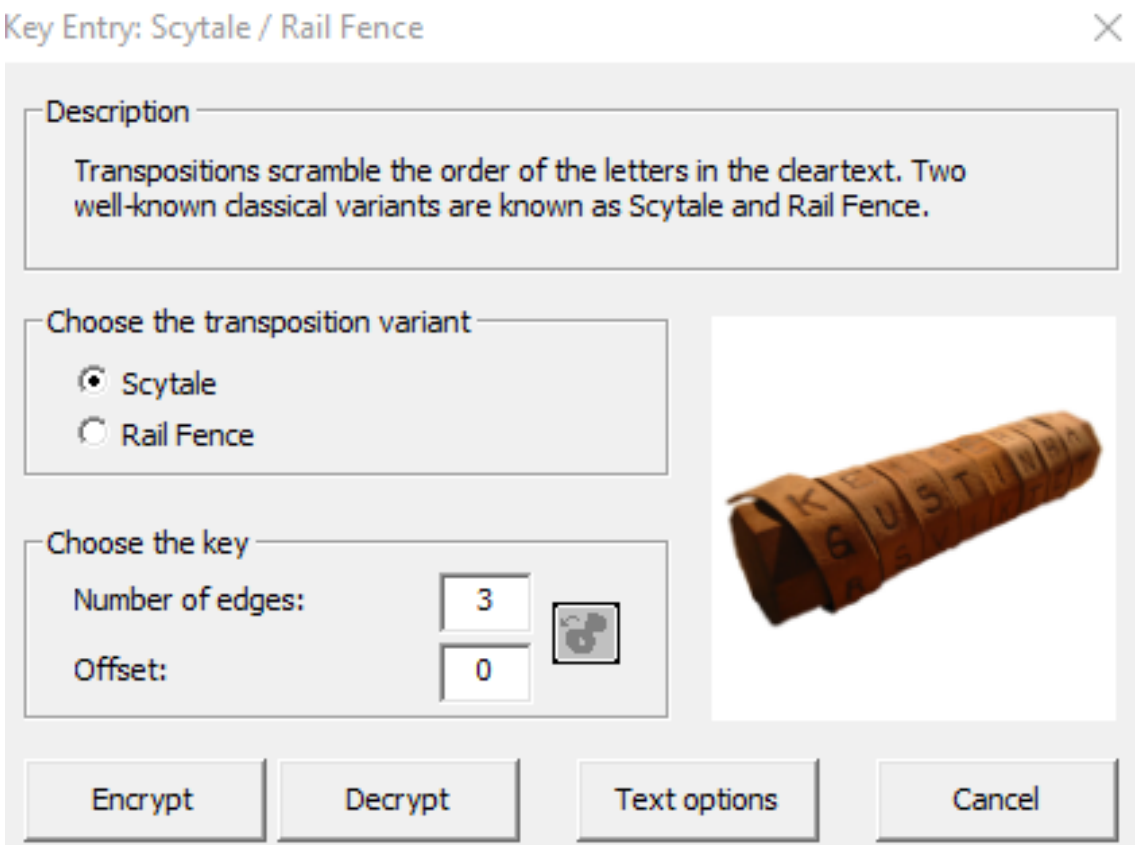
*Задание.*

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.

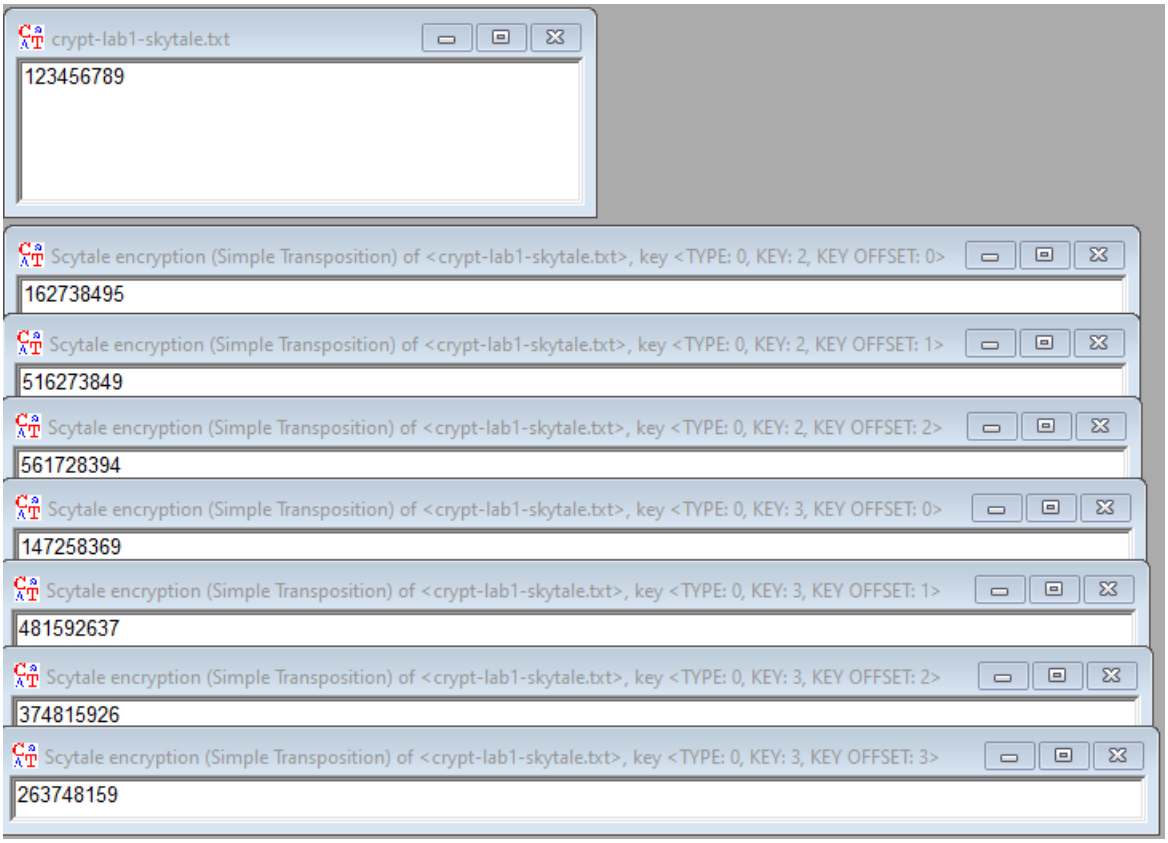
*Реализация в CrypTool 1.*

Для исследования шифра был использован функционал CrypTool 1. Шифр можно найти во вкладке Encrypt/Decrypt -> Symmetric (classic) -> Skytale / Rail Fence.




В качестве открытого текста для исследования работы шифра в зависимости от параметров «Number of Edges» и «Offset» была выбрана последовательность цифр «123456789», так как она поможет отследить перестановку символов в шифротексте.




Было определено, что параметр «Number of Edges» отвечает за количество граней цилиндра, на который «наматывается пергамент» (количество строк в таблице), а параметр «Offset» задает отступ текста от начала.

*Схема, поясняющая работу шифра.*

В криптографии шифр Scytale представляет собой прибор, используемый для осуществления перестановочного шифрования. Прибор состоит из гранёного цилиндра и узкой полоски пергамента, которая обматывается вокруг цилиндра по спирали. На гранях цилиндра записывалось сообщение. Иллюстрация, демонстрирующая работу данного шифра представлена на рисунке 1.1.


*Рисунок 1.1*

Для расшифровки использовался гранёный цилиндр такого же диаметра, на который наматывался пергамент, чтобы прочитать сообщение.

Схему работы шифра можно представить следующим образом. Например, необходимо зашифровать последовательность «123456789» при количестве ребер равному 3 и сдвиге равному 2. Для этого составляется следующая таблица:

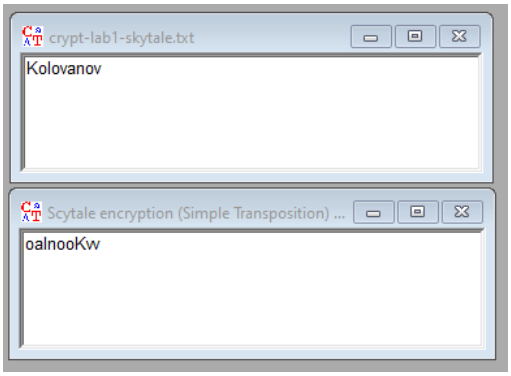
| | | 1 | 2 |
|---|---|---|---|
| 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | |

Здесь количество строк в таблице равно количеству ребер цилиндра, количество пропущенных ячеек в начале таблицы определяется параметром Offset, а количество столбцов выбирается таким образом, чтобы текст вместе с отступом поместился в таблице. Исходный текст записывается по строкам слева направо. Далее если теперь прочитать символы из таблицы по столбцам сверху вниз, то получится шифротекст: «374815926». Дешифрация производится в обратном порядке.

*Пример работы шифра для выбранных параметров.*

Для проверки правильности понимания работы шифра и влияния параметров на результат было выполнено шифрование и дешифрование исходного текста «Kolovanov» вручную и при помощи Cryptool при параметрах «Number of Edges» и «Offset», равных 3.

| | | | K |
|---|---|---|---|
| o | l | o | v |
| a | n | o | v |



В обоих случаях был получен следующий шифротекст: «oalnooKvv».

*Тип шифра.*

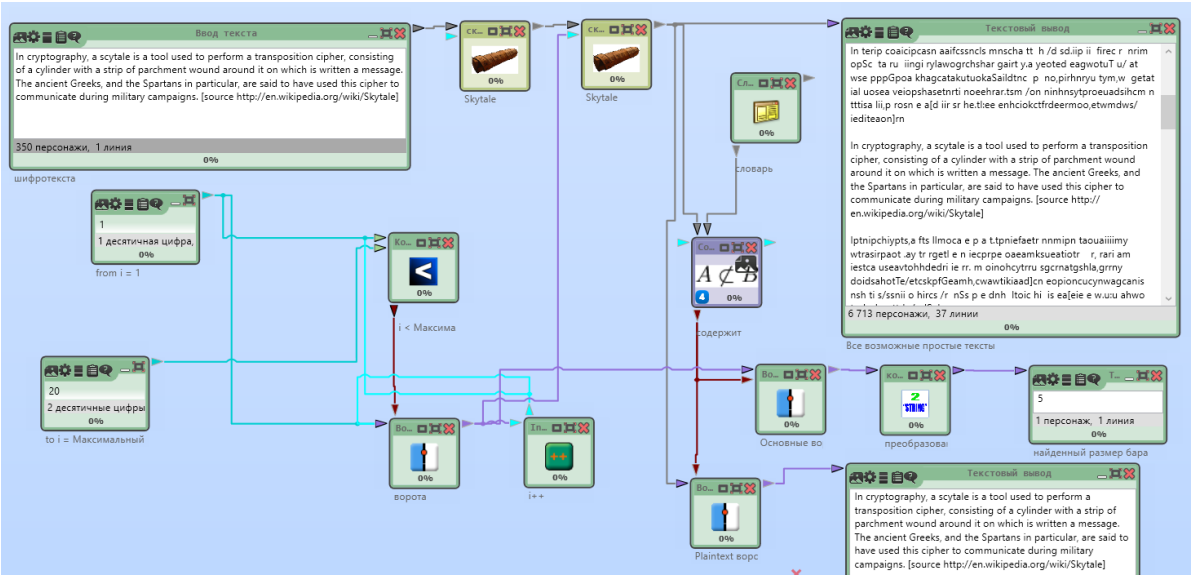
Шифр Skytale является перестановочным.

*Ключ шифра.*

Ключом шифра Skytale являются количество граней цилиндра (количество строк в таблице) и сдвиг текста относительно начала.

*Описание и оценка сложности атаки «грубой силы» на шифротекст, реализованной в CrypTool 2.*

Далее рассмотрим атаку «грубой силой» на шифротекст, реализованную в CrypTool 2, и оценим ее сложность. Ее принцип заключается в том, чтобы расшифровать шифротекст при различных значениях ключа и найти в полученном при расшифровке тексте комбинации символов из словаря. Если расшифрованном тексте их достаточно много, можно сделать вывод, что текст вероятнее всего логически связный, и корректный ключ был найден.




Поскольку количество ребер цилиндра (количество строк) не может превышать количество символов, то сложность атаки не превышает $n^2$, где n – размер сообщения.

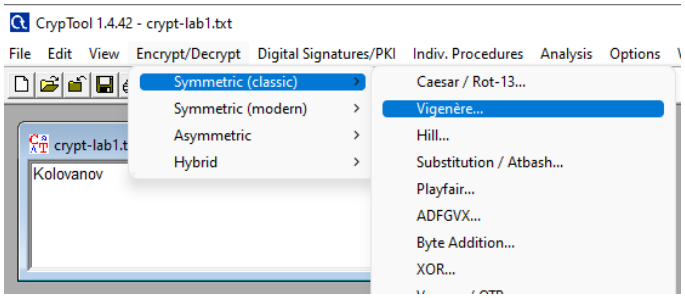
***Шифр Vigenere.***

*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:
    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 изучить атаку, реализованную в CrypTool 2, опираясь на Help и ссылки на статьи.

*Реализация в CrypTool 1.*

Для исследования шифра был использован функционал CrypTool 1. Шифр можно найти во вкладке Encrypt/Decrypt -> Symmetric (classic) -> Vigenere.



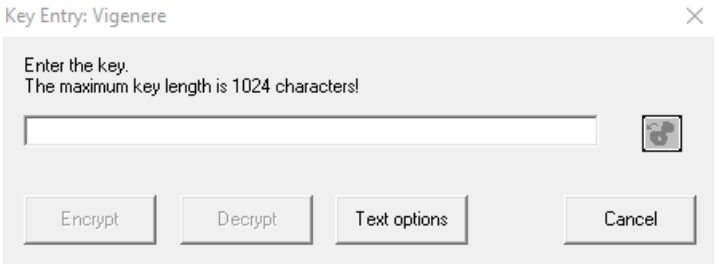



*Схема и формулы, поясняющие работу шифра.*

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, чтобы зашифровать текст *«ПРИМЕРШИФРАВИЖЕНЕРА»*, используя кодовое слово *«КЛЮЧ»* и русский алфавит, необходимо выполнить следующие шаги:

1. Делим текст на отрезки:

| п | р | и | м |
|---|---|---|---|
| к | л | ю | ч |

| е | р | ш | и |
|---|---|---|---|
| к | л | ю | ч |

| ф | р | а | в |
|---|---|---|---|
| к | л | ю | ч |

| и | ж | е | н |
|---|---|---|---|
| к | л | ю | ч |

| е | р | а | |
|---|---|---|---|
| к | л | ю | |

2. Производим замену (для 1-ого отрезка):

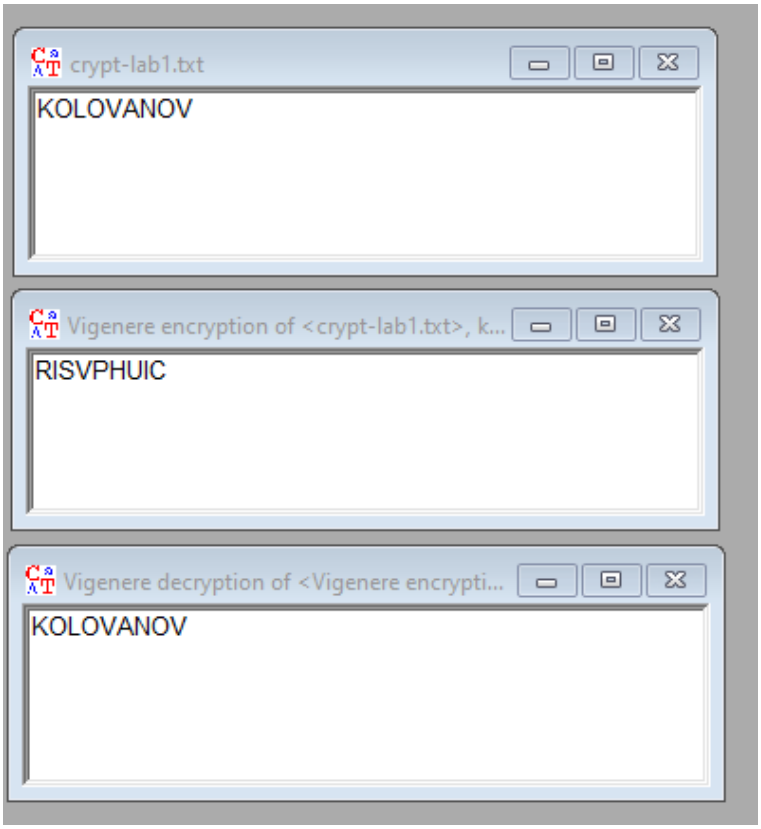
| а | б | в | г | д | е | ж | з | **и** | к | л | **м** | н | о | **п** | **р** | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *К* | л | м | н | о | п | р | с | 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: *«ШЪЖВПЪЦЯЭЪЮЩТСГГПЪЮ»*.

*Пример шифра для выбранных параметров.*

Для проверки понимания работы шифра был зашифрован и после расшифрован текст «KOLOVANOV» при помощи ключа «HUH» вручную и при помощи CrypTool, после чего было проведено сравнение результатов. Шифротекст и расшифрованный текст совпал в обоих случаях:




| K | O | L | O | V | A | N | O | V |
|---|---|---|---|---|---|---|---|---|
| H | U | H | H | U | H | H | U | H |
| R | I | S | V | P | H | U | I | C |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 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 |
| 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 |

Шифротекст: «RISVPHUIC».

Расшифрованный текст: «KOLOVANOV».

*Тип шифра.*

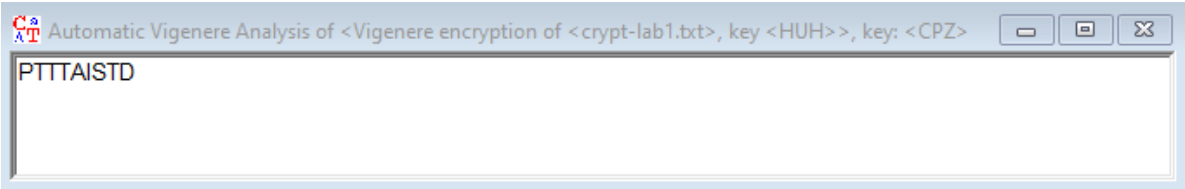
Шифр Виженера является подстановочным.

*Ключ шифра.*

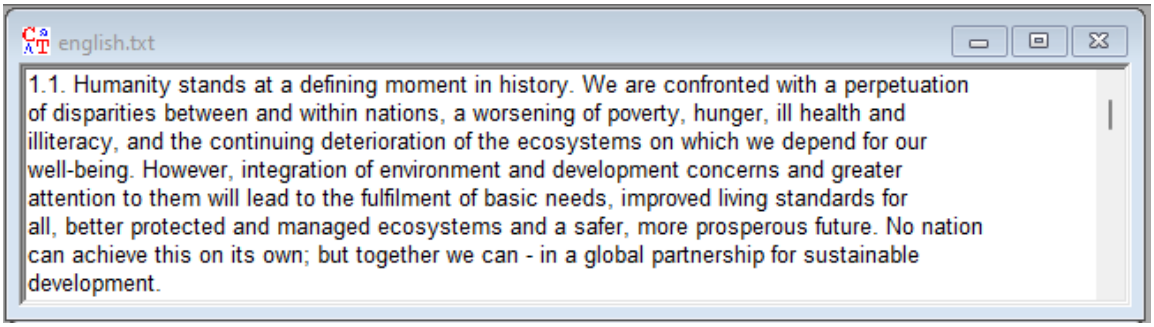
Ключом шифра Виженера является последовательность символов из алфавита.

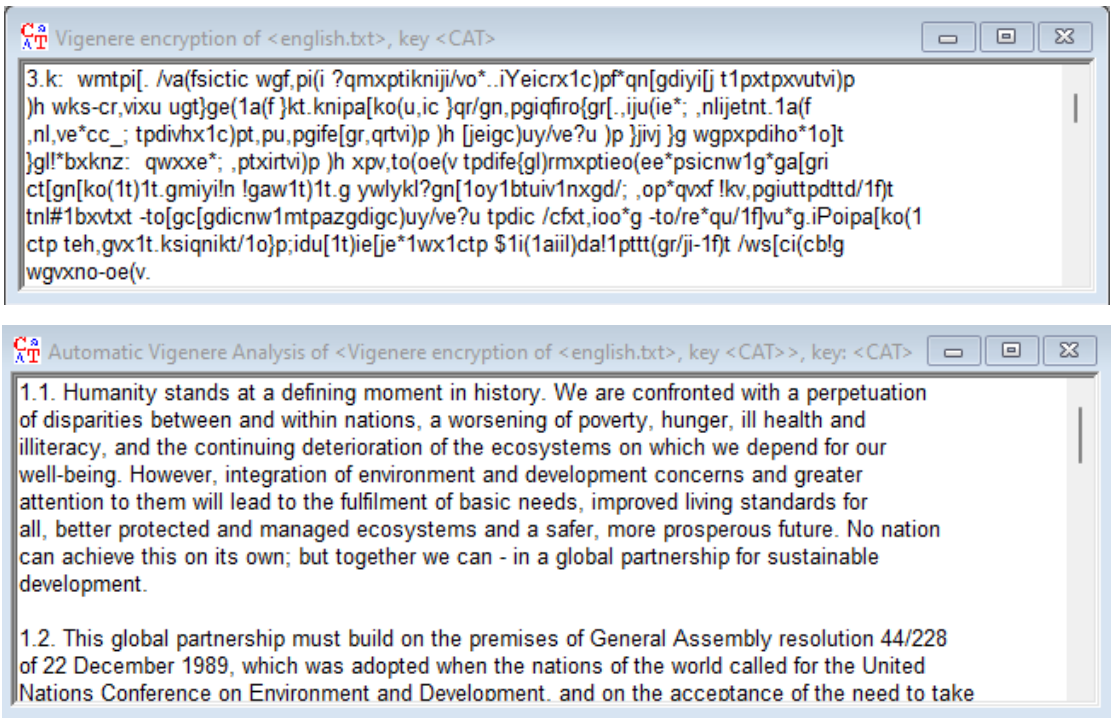
*Описание выполненной процедуры атаки «грубой силы».*

Далее была проведена атака на полученный ранее шифротекст при помощи инструмента Analysis -> Symmetric Encryption (Classic) -> Cipher Text Only -> Vigenere. Полученный при помощи атаки ключ «CPZ» был неверным (правильный ключ – «HUH»). Это можно объяснить слишком малым размером исходного текста – частотный анализ в этом случае дает очень неточные результаты.

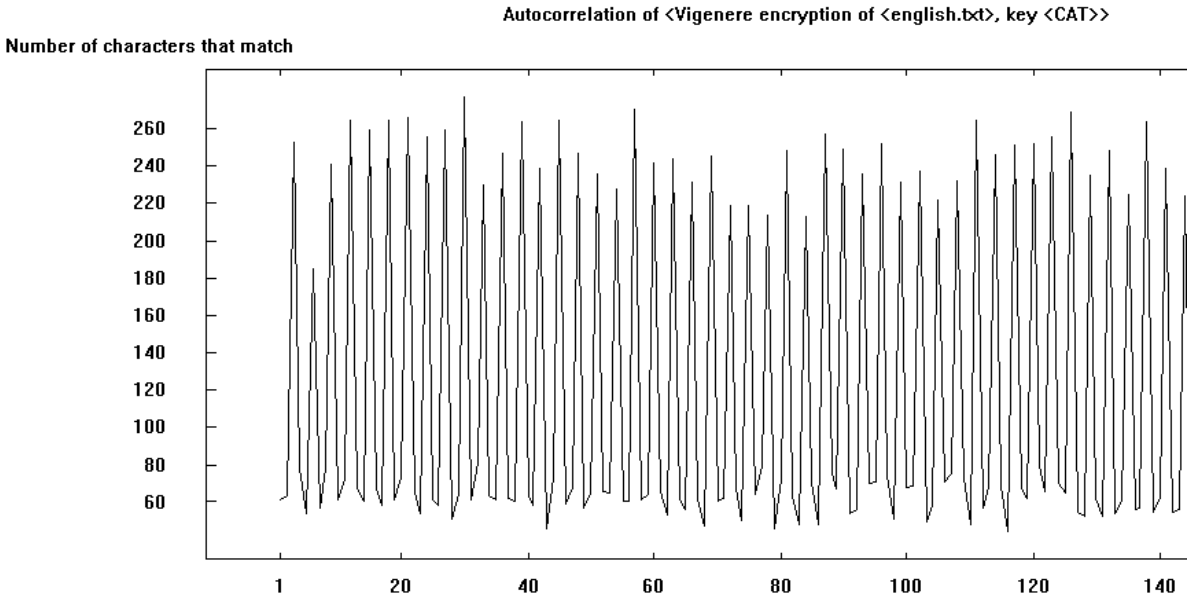



Далее была проведена такая атака на более объемный по размеру фрагмент текста, взятый из файла CrypTool/reference/english.txt. Он был зашифрован при помощи ключа «CAT». Полученный при помощи атаки ключ «CAT» оказался верным:



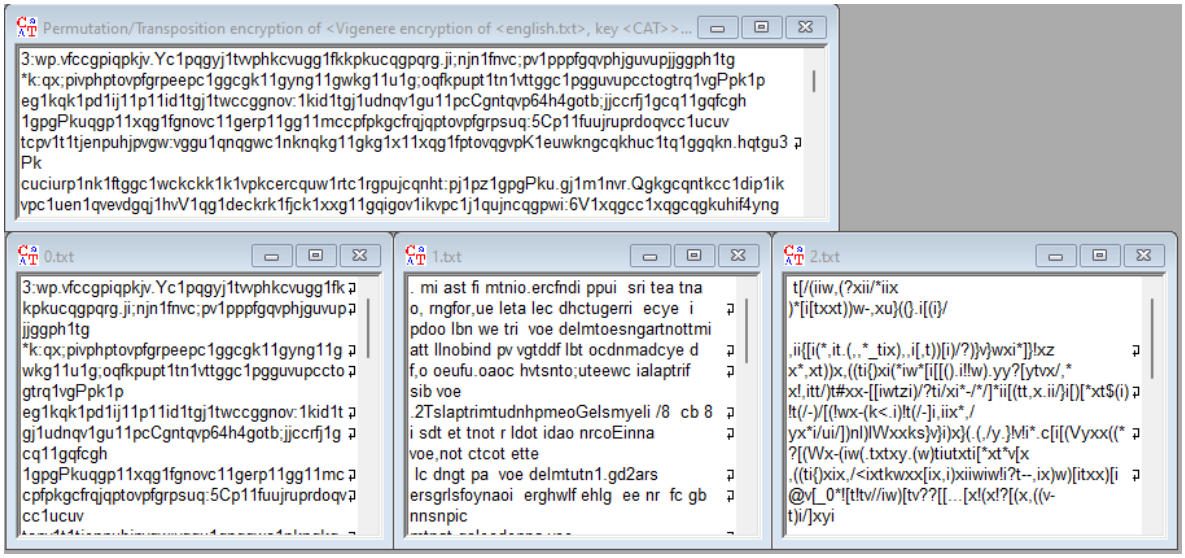



Далее данная атака была воспроизведена в автоматическом режиме. Для начала при помощи инструмента автокорреляции (Analysis -> Tools for Analysis -> Autocorrelation) был найден размер ключа – он равен 3, поскольку на графике наибольшие значения функции достигаются на сдвигах, кратных 3.

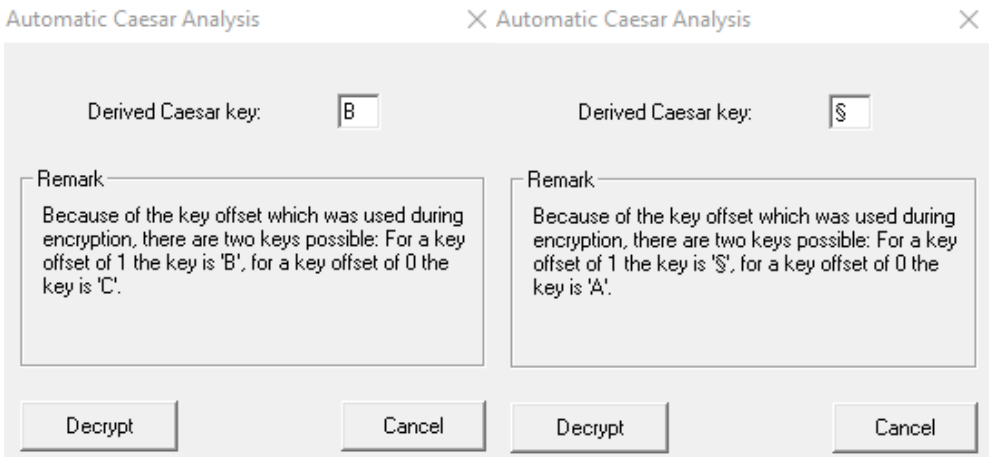


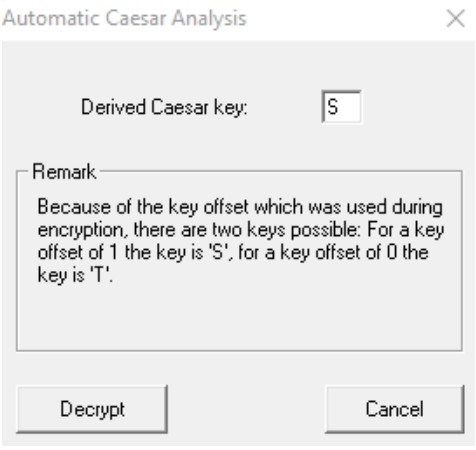

После была выполнена перестановка текста с размером столбца, равным размеру ключа, приложением Permutation/Transposition, чтобы получить части

текста, замена которых осуществлялась при помощи одной и той же буквой ключа. Полученные части представлены в файлах 0.txt, 1.txt и 2.txt.




В конце для каждого из файлов был применён инструмент Analysis -> Symmetric Encryption (Classic) -> Cipher Text Only -> Caesar для атаки на шифр Цезаря:



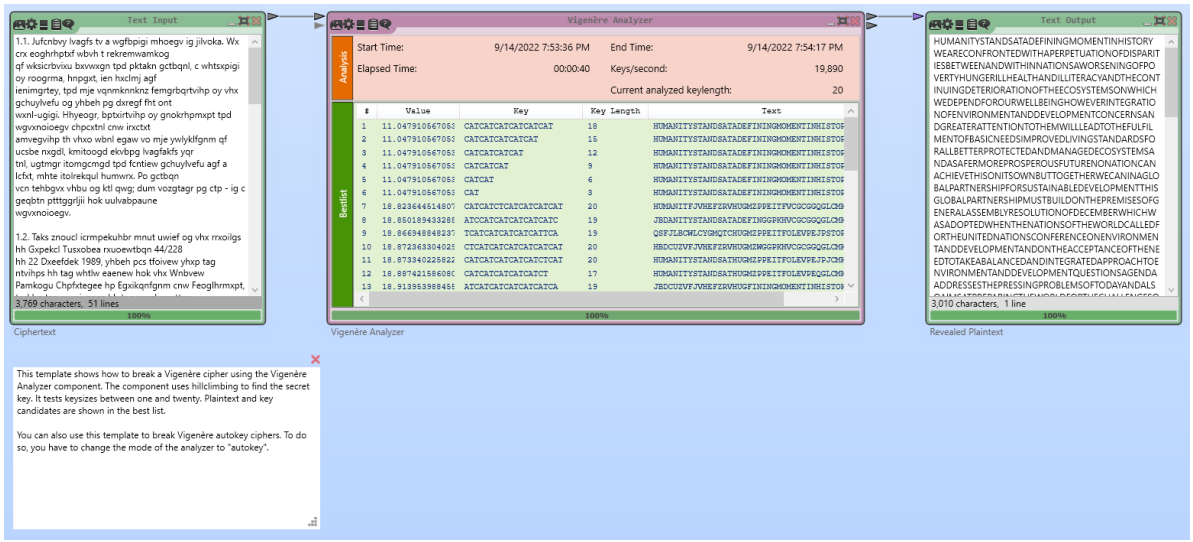
Был получен ключ «B§S». С поправкой на смещение, равное нулю, ключом является «CAT». Полученный ключ совпадает с исходным, атака выполнена успешно.

*Описание сложности атаки «грубой силы».*

Сложность атаки «грубой силы» составляет n! / (n - m)!, где n – это размер алфавита, а m – размер ключа.

*Описание атаки на шифр, реализованной в CrypTool 2.*

Далее рассмотрим атаку «грубой силой», реализованную в CrypTool 2, на шифротекст из предыдущего раздела, зашифрованный ключом «CAT»:




Атака устроена следующим образом. Алгоритм пробегает по различным длинам ключа (в данном случае от 1 до 20), и для каждой длины пытается найти оптимальные ключи. На очередном шаге с фиксированной длиной ключа генерируется случайный ключ и вычисляется его стоимость, после чего происходит попытка его изменения. Для измененной версии также рассчитывается стоимость. Если у измененного ключа стоимость ниже, то он заменяет предыдущий ключ, иначе – предыдущий остается. Происходит это до тех пор, пока ключ можно уменьшить в стоимости, иначе происходит увеличения размера ключа на 1 и процесс повторяется.

***Шифр Hill.***

*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. Передать произвольную шифровку коллеге по учебной группе для расшифрования при условии, что формы обращения и завершения сообщения известны. Размер использованного ключа держать в секрете.

*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 на M и создается шифрующая матрица N на 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.

В качестве примера шифрования, зашифруем 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 |

$$\begin{pmatrix} 7 & 8 & 11 \\ 11 & 2 & 8 \\ 15 & 7 & 4 \\ 17 & 4 & 23 \\ 0 & 12 & 15 \\ 11 & 4 & 18 \end{pmatrix} \times \underbrace{\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}}_{\text{Шифрующая матрица}} = \begin{pmatrix} 366 & 483 & 552 \\ 252 & 432 & 151 \\ 261 & 540 & 145 \\ 614 & 863 & 402 \\ 456 & 447 & 345 \\ 478 & 634 & 321 \end{pmatrix} \equiv \begin{pmatrix} 2 & 15 & 18 \\ 18 & 16 & 21 \\ 1 & 20 & 15 \\ 16 & 5 & 12 \\ 14 & 5 & 7 \\ 10 & 10 & 9 \end{pmatrix} (mod 26)$$

Шифротекст: *«CPSSQVBUPQFMOFHKKJ»*.

Для демонстрации дешифровки, расшифруем полученный 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 |

$$\begin{pmatrix} 2 & 15 & 18 \\ 18 & 16 & 21 \\ 1 & 20 & 15 \\ 16 & 5 & 12 \\ 14 & 5 & 7 \\ 10 & 10 & 9 \end{pmatrix} \times \underbrace{\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}}_{\text{Дешифрующая матрица (обратная)}} = \begin{pmatrix} 709 & 346 & 479 \\ 921 & 470 & 684 \\ 743 & 345 & 550 \\ 485 & 264 & 361 \\ 364 & 194 & 301 \\ 479 & 238 & 382 \end{pmatrix} \equiv \begin{pmatrix} 7 & 8 & 11 \\ 11 & 2 & 8 \\ 15 & 7 & 4 \\ 17 & 4 & 23 \\ 0 & 12 & 15 \\ 11 & 4 & 18 \end{pmatrix} (mod 26)$$

Получаем открытый текст: *«HILLCIPHEREXAMPLES»*.

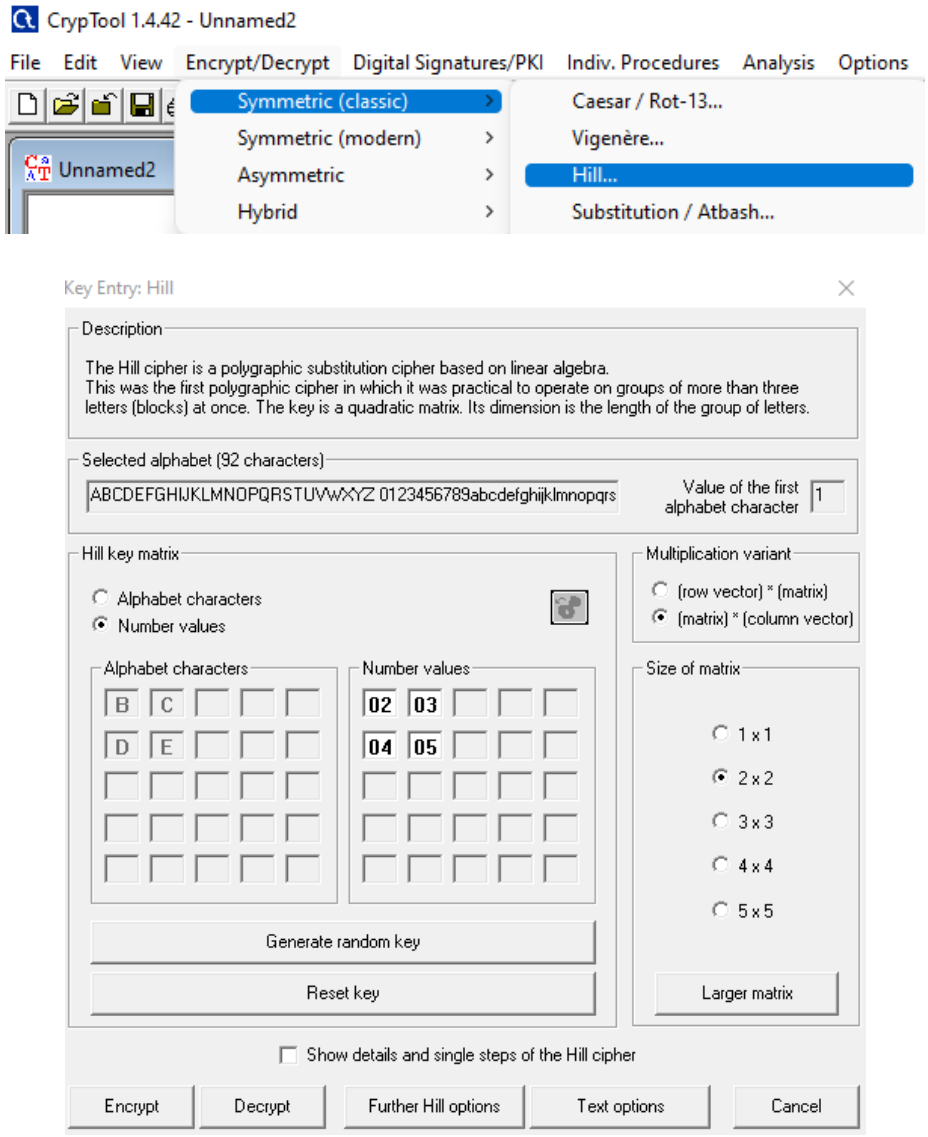
Свойства шифрующей матрицы:

- В общем случае матрица шифрования квадратная m на m, где m – размер блока текста, подлежащего зашифрованию;
- Матрица обратима в том и только в том случае, когда ее детерминант не равен 0 и не имеет общих делителей с основанием модуля;

- Обратная матрица шифрующей матрицы является мультипликативной инверсией M в $Z_{26}$.

*Реализация в CrypTool 1.*

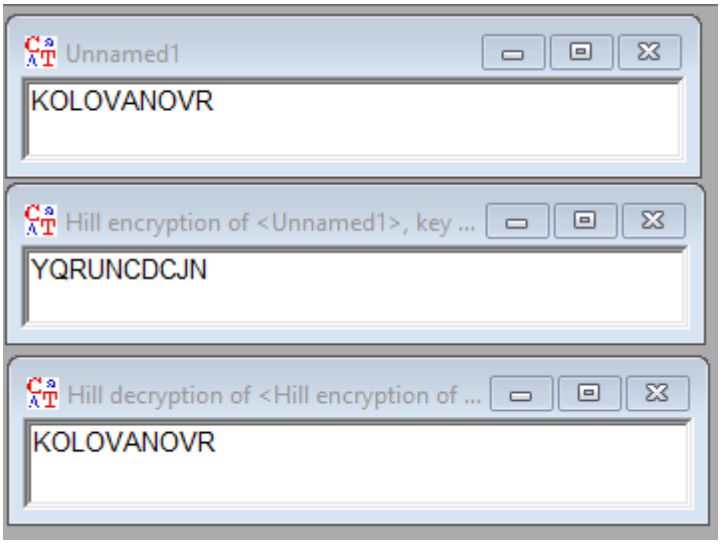
Для исследования шифра был использован функционал CrypTool 1. Шифр можно найти во вкладке Encrypt/Decrypt -> Symmetric (classic) -> Hill.




В качестве основных параметров выступает матрица шифрования/дешифрования, которая задается в таблицах Alphabet Characters или Number Values, ее размер выбирается в пункте Size of matrix.

*Пример работы текста для выбранных параметров и текста сообщения*.

Для проверки правильности понимания работы шифра было выполнено шифрование и дешифрование исходного текста «KOLOVANOVR» вручную и при помощи Cryptool выбранным ключом 2 на 2.




| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| A | --> | 01 | H | --> | 08 | O | --> | 15 | U | --> | 21 |
| B | --> | 02 | I | --> | 09 | P | --> | 16 | V | --> | 22 |
| C | --> | 03 | J | --> | 10 | Q | --> | 17 | W | --> | 23 |
| D | --> | 04 | K | --> | 11 | R | --> | 18 | X | --> | 24 |
| E | --> | 05 | L | --> | 12 | S | --> | 19 | Y | --> | 25 |
| F | --> | 06 | M | --> | 13 | T | --> | 20 | Z | --> | 26 |
| G | --> | 07 | N | --> | 14 | | | | | | |

Матрица шифрования:

| | |
|---|---|
| 19 | 12 |
| 04 | 19 |

Матрица исходного текста:

| | |
|---|---|
| 11 | 15 |
| 12 | 15 |
| 22 | 1 |
| 14 | 15 |
| 22 | 18 |

Для шифровки необходимо умножить матрицу исходного текста на транспонированную матрицу шифрования, после чего взять значения по модулю размера алфавита (26). Получаем следующий шифротекст:

| | |
|---|---|
| 25 | 17 |
| 18 | 21 |
| 14 | 3 |
| 4 | 3 |
| 10 | 14 |

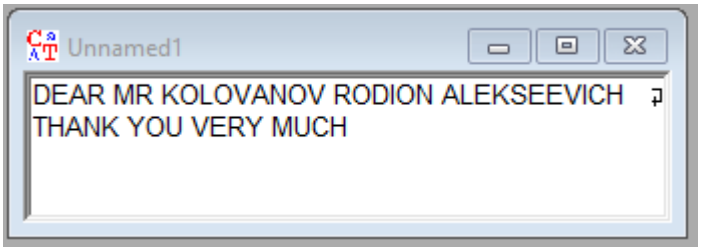
Определитель матрицы шифрования равен 1197 > 0 и не имеет общих делителей с размером алфавита, равным 92. Отсюда существует матрица дешифрования.

Матрица дешифрования:

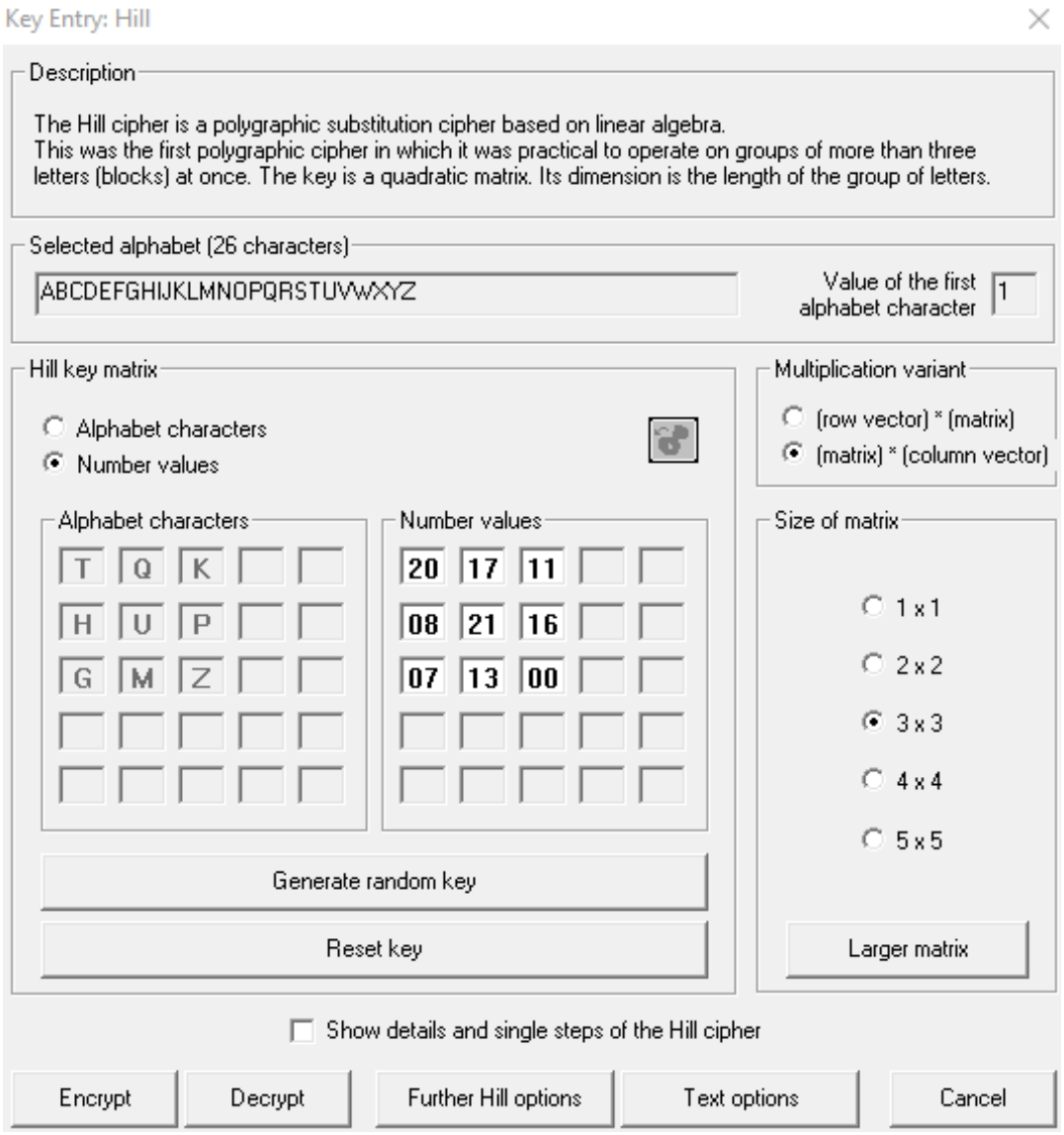
| | |
|---|---|
| 19 | 14 |
| 22 | 19 |

Для расшифровки шифротекста необходимо умножить матрицу шифротекста на транспонированную матрицу дешифрования, после чего взять значения по модулю размера алфавита (26). Получаем следующий расшифрованный текст: «KOLOVANOVR».

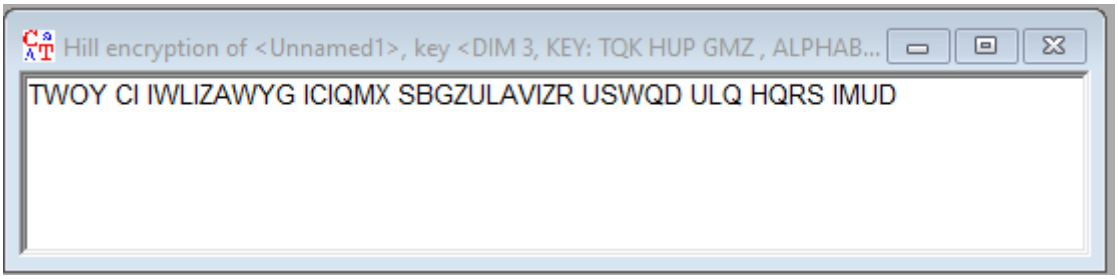
Далее был зашифрован текст с сообщением «DEAR MR KOLOVANOV RODION ALEKSEEVICH THANK YOU VERY MUCH», используя шифрующую матрицу 3 на 3.



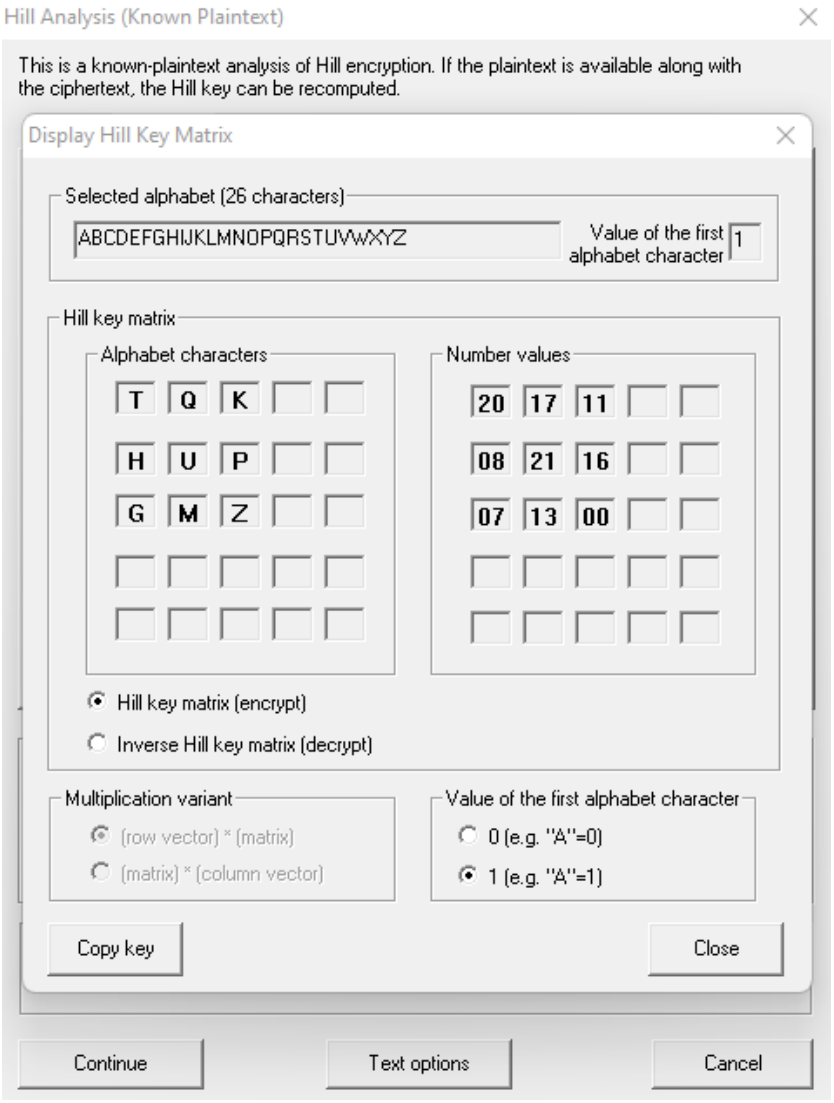

Матрица шифрования и алфавит представлены на следующем изображении:



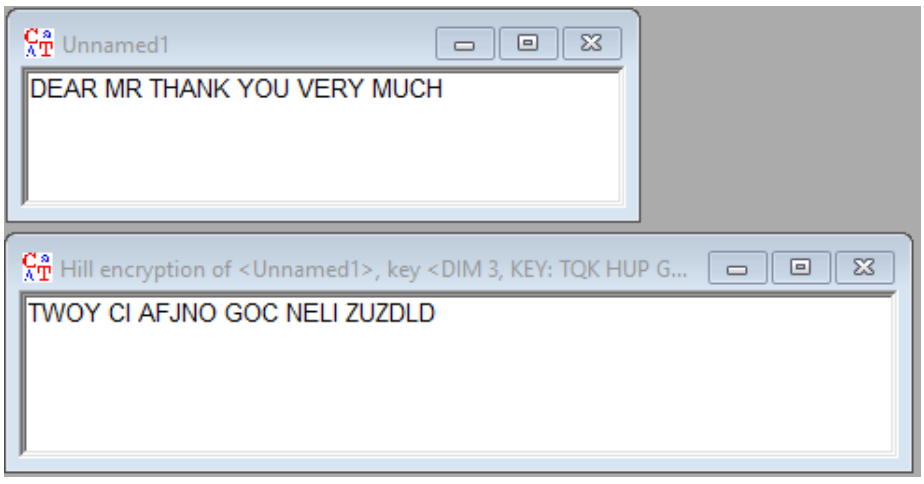

Полученный шифротекст:

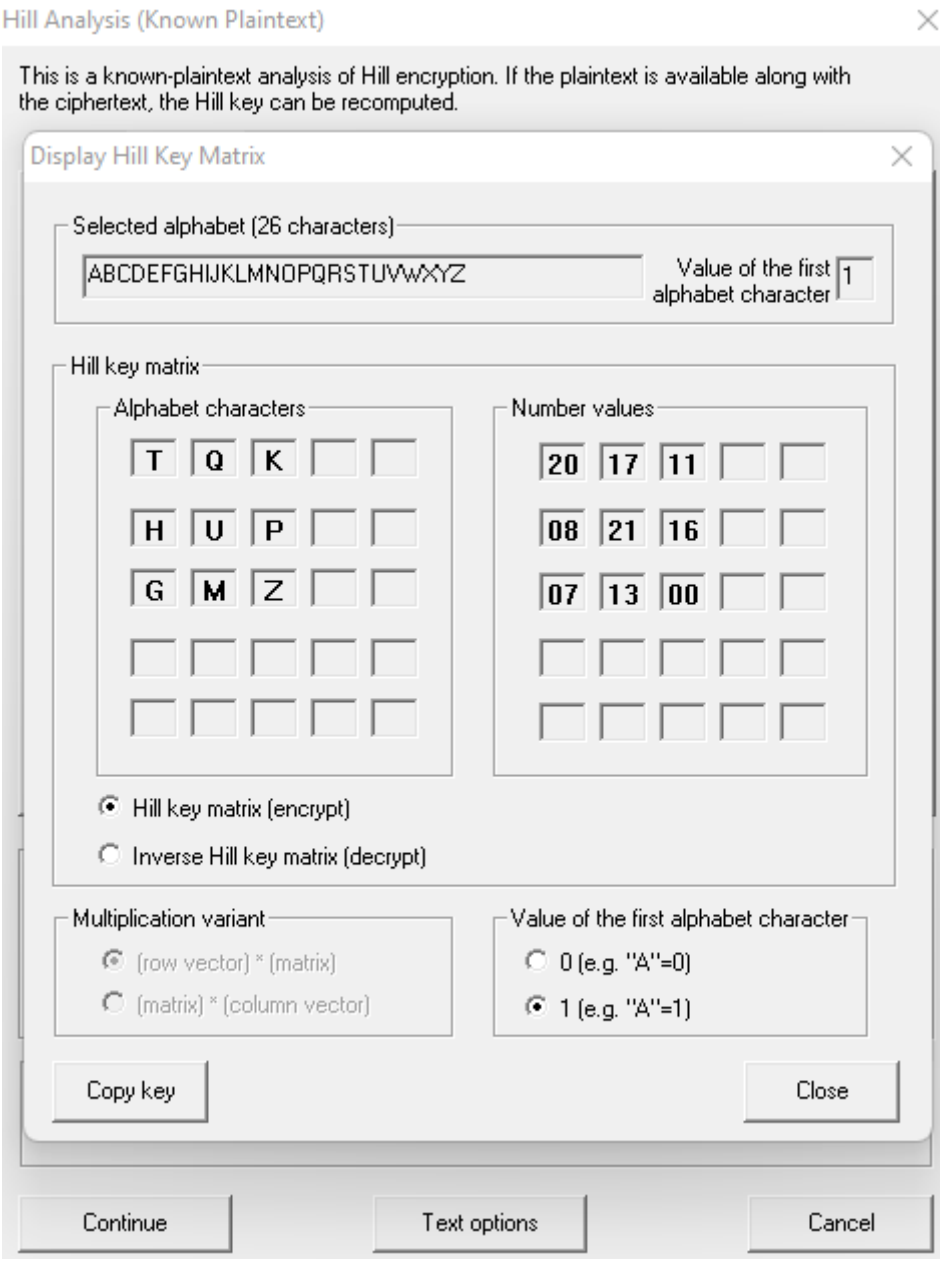



Далее была выполнена атака на основе знания открытого текста, используя инструмент Analyse -> Symmetric Encryption (classic) -> Known Plaintext -> Hill:




Атака прошла успешно, была получена шифрующая матрица, которой производилась шифровка исходного сообщения. Далее из сообщения и шифротекста были убраны фрагменты с фамилией, именем и отчеством, и атака была повторена:






Атака прошла успешно, была получена шифрующая матрица, которой производилась шифровка исходного сообщения.

Коллеге по группе была передана следующая шифровка: «HELLO FRIEND SERGEY TARZANICH CHI KAK LIANA MEET YOU TOMORROW».

*Тип шифра*.

Шифр Хилла является подстановочным, блочным.

*Ключ шифра.*

Ключом шифра Хилла является матрица, имеющая мультипликативную инверсию в кольце по модулю размера алфавита

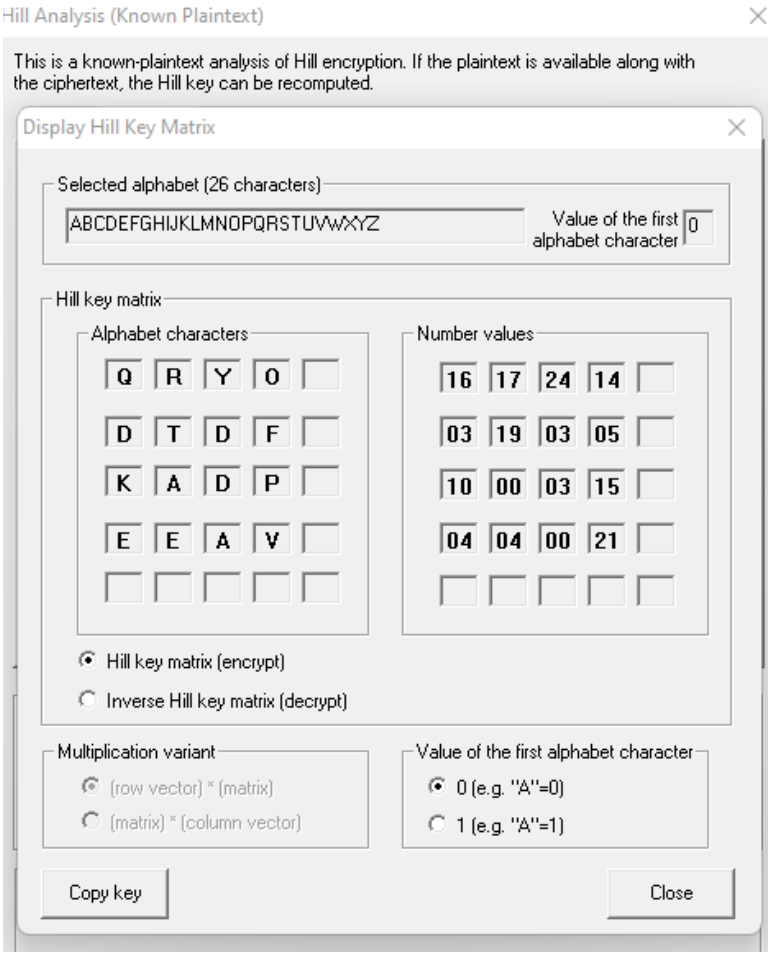
*Оценка сложности атаки «грубой силы».*

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

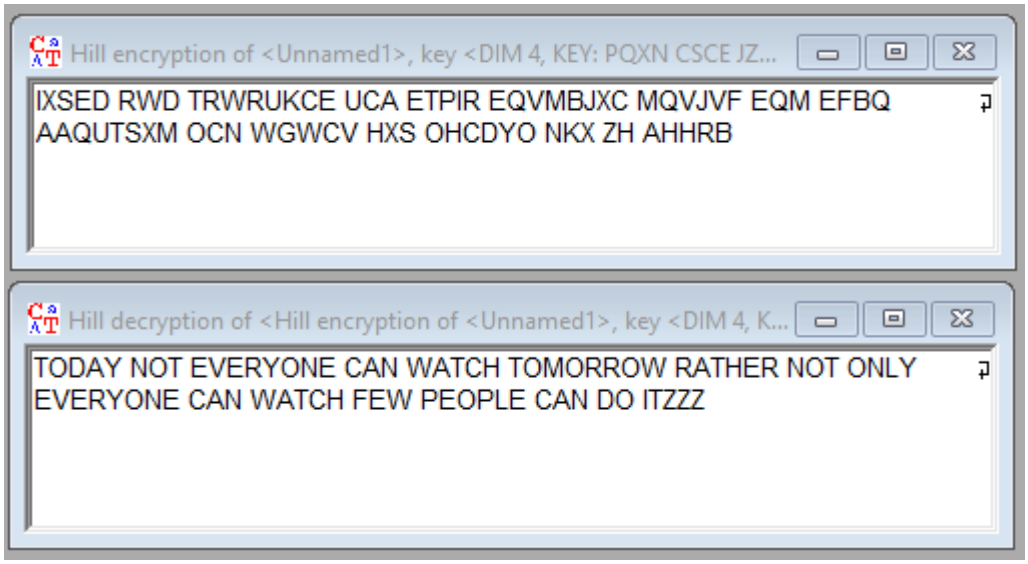
*Результат атаки и расшифровка перехваченного от коллеги текста.*

От коллеги был получен шифротекст «IXSED RWD TRWRUKCE UCA ETPIR EQVMBJXC MQVJVF EQM EFBQ AAQUTSXM OCN WGWCV HXS OHCDYO NKX ZH AHHRB», а также начало и конец исходного текста: «TODAY NOT EVERYONE» и «PEOPLE CAN DO IT» соответственно.

Для начала из шифротекста была вырезана середина, которая не содержит известные части исходного текста. Далее была произведена расшифровка и получена предполагаемая шифрующая матрица размера 4 на 4:



Далее при помощи полученной шифрующей матрицы была осуществлена расшифровка шифротекста, был получен исходный текст «TODAY NOT EVERYONE CAN WATCH TOMORROW RATHER NOT ONLY EVERYONE CAN WATCH FEW PEOPLE CAN DO IT»:



**Выводы.**

В процессе выполнения данной лабораторной работы были изучены шифры Scytale, Vigenere, Hill, а также принципы атаки методом «грубой силы» на исследуемые шифры.

Для шифра Сцитала было определено:

- Параметр «Number of Edges» отвечает за количество граней цилиндра, на который «наматывается пергамент» (количество строк в таблице), а параметр «Offset» задает отступ текста от начала (количество пустых ячеек в таблице перед началом текста);
- Шифровка происходит при помощи записи исходного текста по строкам в таблицу, шифротекст получается при считывании символов по столбцам таблицы;
- Шифр является перестановочным;
- Ключом шифра являются количество граней цилиндра (количество строк в таблице) и сдвиг текста относительно начала;
- Атака происходит при помощи перебора количества граней и значения сдвига. Успешность определяется по количеству совпадающих слов из словаря, которые содержаться в расшифрованном тексте.
- Сложность атаки «грубой силы» не превышает $n^2$, где n – размер сообщения.

Для шифра Виженера было определено:

- Для шифрования/расшифрования формируется гамма повторения ключа $G = (K_1,\ldots,K_m)\ldots(K_1,\ldots,K_m)$, шифровка и расшифровка происходит следующим образом: $C_i = (P_i + G_i) \bmod n$ и $P_i = (C_i - G_i) \bmod n$ соответственно;
- Шифр является подстановочным;
- Ключом шифра является последовательность символов из алфавита;

- Атака происходит в два этапа: в первом определяется размер ключа при помощи автокорреляционного метода, во втором – происходит разбиение текста на группы символов, зашифрованные одним и тем же алфавитом (одним и тем же символом ключа), после чего используется атака на шифр Цезаря для каждой из групп;
- Атаку с использованием частотного анализа можно применять в случае достаточно большого размера текста;
- Сложность атаки «грубой силы» составляет n! / (n - m)!, где n – это размер алфавита, а m – размер ключа.

Для шифра Хилла было определено:

- Шифровка осуществляется при помощи представления исходного текста в виде матрицы, после чего осуществляется перемножение с шифрующей матрицей, значения берутся по модулю размера алфавита;
- Расшифровка происходит аналогичным образом, только вместо шифрующей матрицы используется расшифровывающая матрица, которая является мультипликативной инверсией шифрующей матрицы в кольце вычетов по модулю размера алфавита;
- Шифр является блочным подстановочным;
- Ключом шифра является матрица, имеющая мультипликативную инверсию в кольце вычетов по модулю размера алфавита;
- Атака происходит с учетом знания некоторой части исходного текста. Перебираются размеры шифрующей матрицы и выполняется попытка восстановить шифрующую матрицу по блокам исходного текста и шифротекста;
- Сложность атаки методом «грубой силы» составляет в худшем случае $n^{m*m}$.

Были получены практические навыки работы с перечисленными шифрами. Для каждого из шифров производилась шифровка исходного текста, расшифровка шифротекста, атака на шифротекст методом «грубой силы», в том числе с использованием приложений Cryptool 1 и 2.