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

ОТЧЕТ

по лабораторной работе №1-2-3

по дисциплине «Криптография и защита информации»

Тема: Изучение классических шифров. Вариант №7: шифры Изгородь, Виженера, Хилла.

Студент гр. 0303 _____ Калмак Д.А.

Преподаватель _____ Племянников А.К.

Санкт-Петербург

2023

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.

Порядок выполнения работы.

1. Описать схему процесса зашифрования и расшифрования сообщения.

2. Описать характеристики шифра: способ обработки символов сообщения (блочность), виды используемых операций над символами, определение ключа шифра в исследуемой реализации.

3. Математически вывести оценку асимптотической сложности атаки "грубой силы".

4. Выполнить и описать атаку на шифровку.

Выполнение работы.

1. Шифр «Изгородь» (Rail Fence)

1.1 Схема процесса зашифрования и расшифрования сообщения

Шифр «Изгородь» использует таблицу-шаблон, которая содержит заданное количество строк, равное высоте изгороди. Открытый текст вписывается в эту таблицу построчно, причем каждая буква записывается в строку с определенным смещением от левого края шаблона, как если бы это была изгородь. Затем зашифрованный текст создается путем объединения символов из разных строк таблицы-шаблона. Например, если взять открытый текст "0123456789" и поместить его в шаблон из трех строк, шифротекст будет выглядеть так: "0481357926". (см. рис. 1)

0	x	x	x	**4**	x	x	x	**8**	x
x	**1**	x	**3**	x	**5**	x	**7**	x	**9**
x	x	**2**	x	x	x	**6**	x	x	x

Рисунок 1 – Результат шифрования без смещения

Чтобы расшифровать, необходимо вписать шифротекст в исходную таблицу-шаблон и затем выполнить действия в обратном порядке, чтобы получить исходный открытый текст.

Для увеличения криптостойкости этого шифра можно ввести смещение при записи открытого текста в таблицу-шаблон. Например, если применить смещение 2 и выполнить шифрование с тем же открытым текстом "0123456789" в таблице из трех строк, то шифротекст будет выглядеть так: "2613579048". (см. рис. 2)

-	x	x	x	2	x	x	x	6	x	x	x
x	-	x	1	x	3	x	5	x	7	x	9
x		0	x	x	x	4	x	x	x	8	x

Рисунок 2 – Результат шифрования со смещением 2

С использованием программы Cryptool 1 проведено шифрование текста – “0123456789” с высотой изгороди 4 и смещением 2, и получен шифротекст – “4359026817”, затем проведено расшифрование. (см. рис. 3)

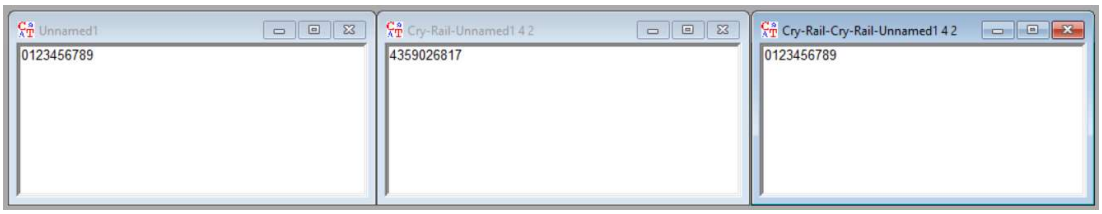

Рисунок 3 – Проведение шифровки и расшифровки в Cryptool 1, используя шифр «Изгородь»

1.2 Характеристики шифра

Шифр “Изгородь” перестановочный. Для его шифровки и расшифровки используется ключ с числами k, m, где k – число, соответствующее высоте изгороди, а m – число, соответствующее смещению. При этом шифр не является блочным, так как в этом шифре открытый текст полностью вписывается в таблицу-шаблон.

1.3 Оценка асимптотической сложности атаки "грубой силы"

Атака “грубой силы” заключается в переборе всех ключей. Ключ для шифра Изгородь состоит из двух чисел: высота изгороди k и смещение m. Высота изгороди должно быть больше единицы, также высота должна быть меньше длины исходного текста, так как иначе шифротекст будет совпадать с исходным текстом. То есть $k \in [2, n-1]$, где n – длина исходного текста. Сдвиг имеет ограничение снизу 0, когда 0, то сдвига нет. У сдвига есть период, то есть сдвигая, после определенного значения шифротекст начнет повторяться. Расстояние от верхней части изгороди до нижней и от нижней до верхней равно по $k-1$, то есть вместе $2k-2$, но сдвиг $2k-2$ повторяет 0, поэтому верхняя граница $2k-3$. То есть $m \in [0, 2k-3]$.

$$O(n) = \sum_{k=2}^{n-1} \sum_{m=0}^{2k-3} 1 \approx n^2$$

Асимптотическая сложность атаки "грубой силы" n^2.

1.4 Атака на шифровку

Атака на шифр изгородь, который является перестановочным, заключается в переборе всех ключей до сообщения, которое имело бы смысл. Атака на шифротекст с исходным текстом KALMAK с высотой изгороди 3 и смещением 2 представлена на рис. 4.

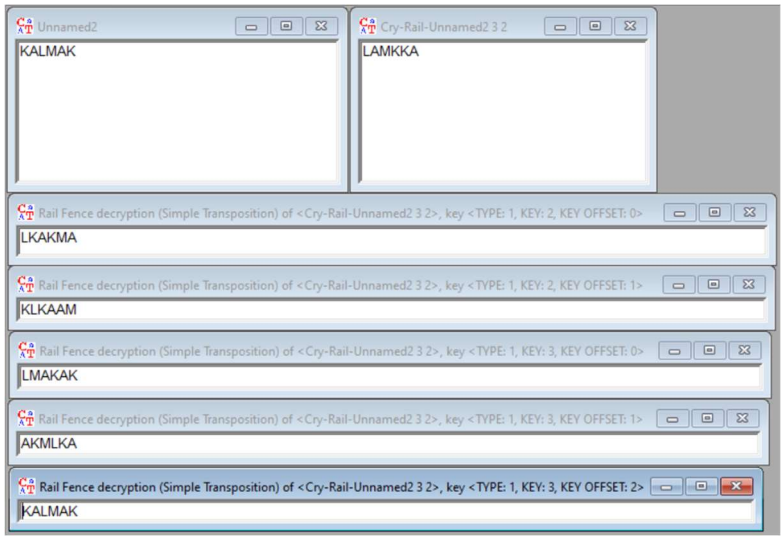

Рисунок 4 – Атака на шифр изгородь

2. Шифр Виженера (Vigenere)

2.1 Схема процесса зашифрования и расшифрования сообщения

Для зашифрования используется таблица замен. Каждой букве алфавита исходного сообщения сопоставляются несколько вариантов букв для представления в шифротексте. Сначала выбирается кодовое слово длиной n, которое разбивает открытый текст на сегменты такой же длины. Затем создается таблица Виженера, которая выглядит следующим образом: алфавит исходного языка записывается горизонтально, а под первой буквой алфавита вертикально записывается кодовое слово. Заполнение таблицы происходит путем вписывания символов алфавита, начиная с буквы, соответствующей следующей букве кодового слова и циклически возвращаясь к началу алфавита. Например, в латинском алфавите после xyz пойдет латинский алфавит с начала, то есть abc… Для получения элемента шифротекста выбирается пересечение столбца, соответствующего букве открытого текста, и строки, соответствующей букве кодового слова.

Например, исходный текст «примершифравиженера». За n принято 4 и за ключ взято слово «ключ». Полученное разделение исходного текста представлено на рис. 5.

п	р	и	м	е	р	ш	и	ф	р	а	в	и	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	

Рисунок 5 – Разделение текста на отрезки

По таблице Виженера сопоставляются символы для шифротекста: пересечение “п” и “к” – “ш”, “р” и “л” – “ъ”, “и” и “ю” – “ж”, “м” и “ч” – “в”. (см. рис. 6)

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	и
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

Рисунок 6 – Замена для первого отрезка

Заменив все отрезки аналогичным образом, шифротекст будет иметь вид “шъжвпъцяэъющтсггпъю”.

Для расшифровки шифротекст также разбивается на сегменты. Для получения символа исходного сообщения выбирается символ из первой строки, находящийся в столбце, соответствующем текущему символу шифротекста, который пересекается со строкой, соответствующей текущему символу ключа.

С использованием программы Cryptool 2 проведено шифрование текста с ключом “SECRETKEY” и проведено расшифрование. (см. рис. 7)

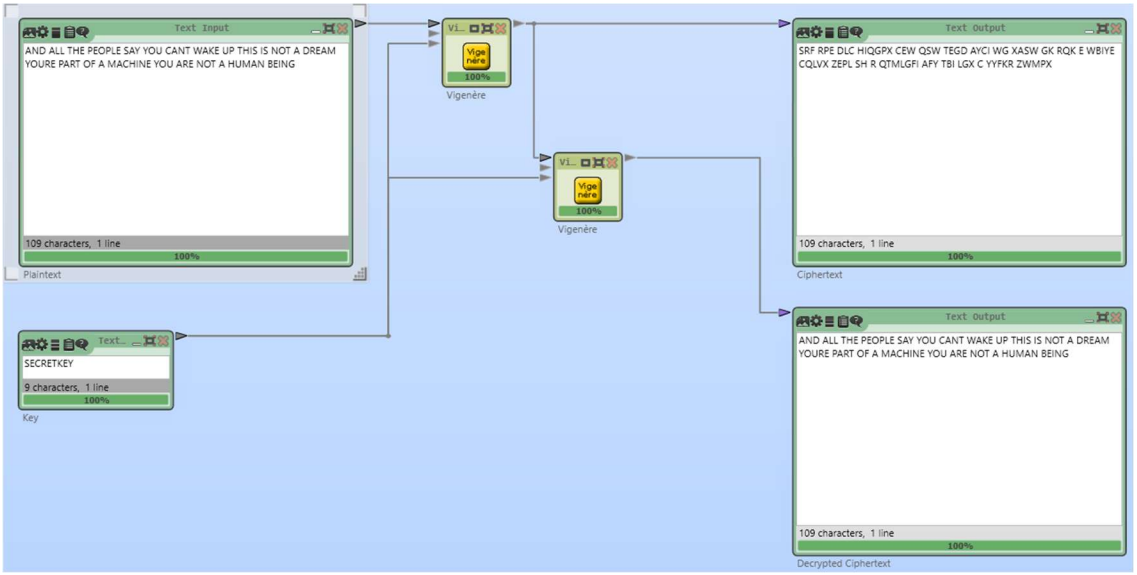

Рисунок 7 – Проведение шифровки и расшифровки в Cryptool 2, используя шифр Виженера

2.2 Характеристики шифра

Шифр Виженера - многоалфавитный шифр замены. Для шифра Виженера ключ состоит из слова, состоящего из символов алфавита. Для шифрования и расшифровки сообщение разбивается на блоки соразмерные с ключом – шифр блочный. Замена символов происходит по таблице Виженера.

2.3 Оценка асимптотической сложности атаки "грубой силы"

Атака “грубой силы” заключается в переборе всех ключей: перебор всех длин ключей, причем длина ключа не может превосходить длину исходного текста, а также перебор всех комбинаций символов в ключах этих длин. Длина ключа от 1 до n, где n – длина исходного текста.

$O(n) = \sum_{k=1}^{n} A^k$, где k – длина ключа, A - длина алфавита.

Тогда асимптотическая сложность атаки "грубой силы" A^n, где A - длина алфавита.

2.4 Атака на шифровку

Атака на шифр Виженера проведена с использованием Cryptool 2 и представлена на рис. 8. Исходный текст AND ALL THE PEOPLE SAY YOU CANT WAKE UP THIS IS NOT A DREAM YOURE PART OF A MACHINE YOU ARE NOT A HUMAN BEING совпадает с дешифрованным текстом за исключением пробелов.

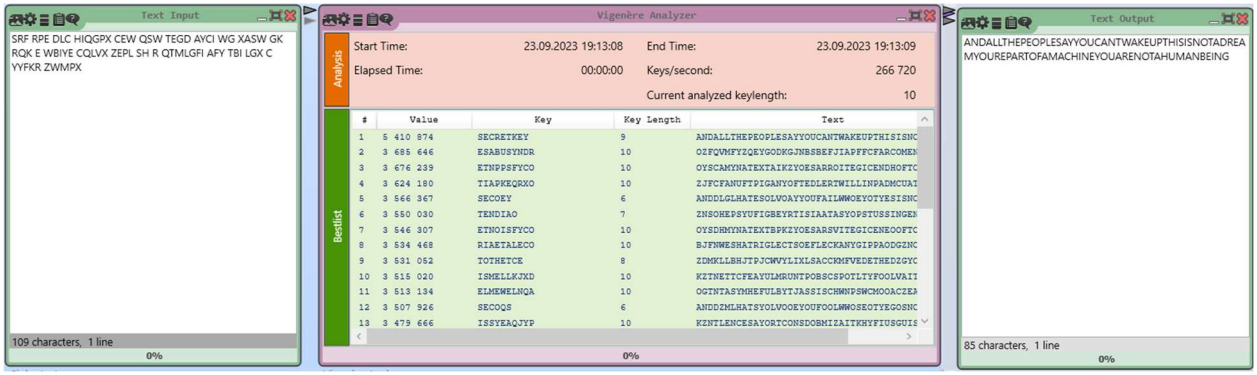

Рисунок 8 – Атака на шифр Виженера

3. Шифр Хилла (Hill)

3.1 Схема процесса зашифрования и расшифрования сообщения

Шифр Хилла оперирует матричным преобразованием текста. Сначала каждому символу алфавита присваивается код, соответствующий его порядковому номеру в алфавите. Затем эти коды символов открытого текста помещаются в матрицу размером n × m, а также создается шифрующая

матрица n × n. Для выполнения шифрования матрица открытого текста умножается на шифрующую матрицу, и затем вычисляется остаток от деления значений элементов получившейся матрицы-произведения на число символов в выбранном алфавите. Для расшифровки необходимо умножить шифротекст на матрицу, которая является обратной к шифрующей матрице.

Например, зашифруем “hillcipherexamples”. Латинский алфавит состоит из 26 символов, каждому символу присвоен код от 0 до 25. Матрица исходного текста размером 3 на 6, шифрующая матрица 3 на 3. Перемножив матрицы и взяв остаток от 26, получен шифротекст “cpssqvbupqfmofhkkj” (см. рис. 9)

Рисунок 9 – Шифрование текста шифром Хилла

Расшифруем полученный шифротекст “cpssqvbupqfmofhkkj”. Соответствие символов алфавита и их кодов то же. Умножив матрицу шифротекста размером 3 на 6 на дешифрующую матрицу (обратную к шифрующей матрице) размером 3 на 3, получена матрица исходного текста. (см. рис. 10)

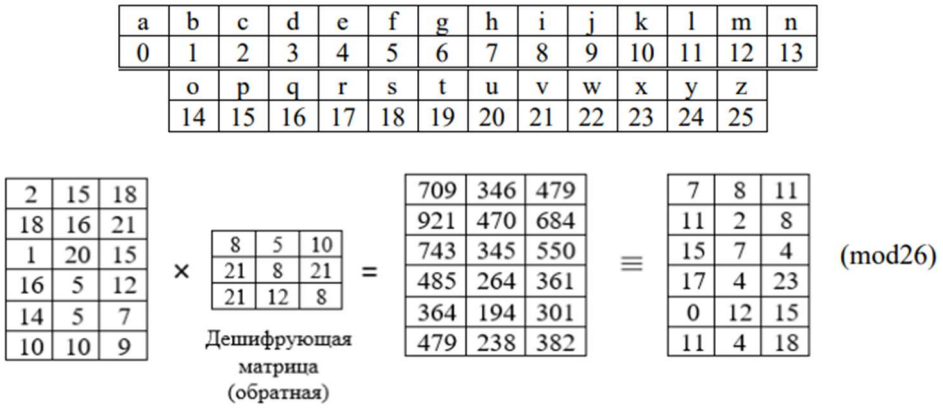

Рисунок 10 – Расшифровка шифра Хилла

С использованием программы Cryptool 2 проведено шифрование текста

$$\begin{matrix} 2 & 15 & 22 \\ 1 & 9 & 1 \\ 16 & 7 & 13 \end{matrix}$$

с ключом и проведено расшифрование. (см. рис. 11)

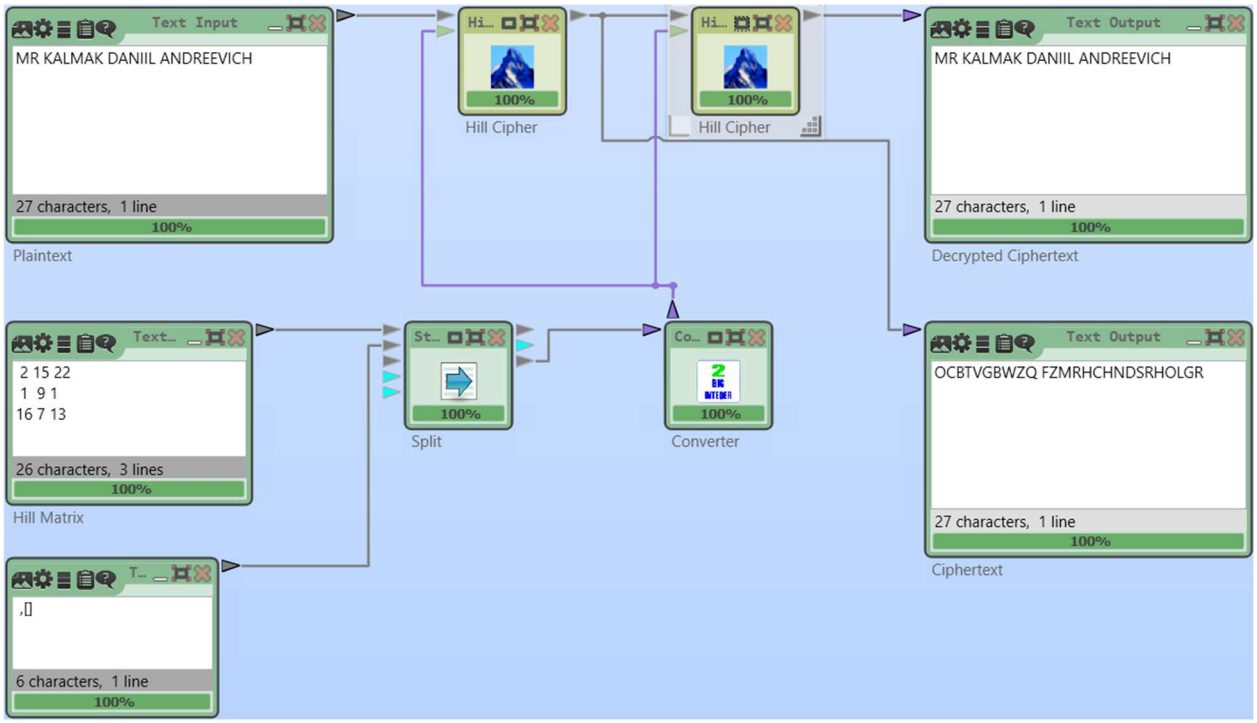

Рисунок 11 – Проведение шифровки и расшифровки в Cryptool 2, используя шифр Хилла

3.2 Характеристики шифра

Шифр Хилла — это шифр многоалфавитной замены, но с математическим подходом к шифрованию и дешифрованию. Символы заменяются на цифровое соответствие, а затем заполняются в матрицу блочно, шифр является блочным. Для шифровки и дешифровки матрица умножается на ключ. Ключ шифра Хилла представляет собой квадратную матрицу, размер которой определяется длиной блока символов. Эта матрица должна быть обратимой, чтобы обеспечить возможность дешифрования.

3.3 Оценка асимптотической сложности атаки "грубой силы"

Атака “грубой силы” заключается в переборе всех ключей: перебор всех матриц размера n на n, каждый элемент матрицы может принимать любое значение из алфавита длиной A.

$$O(n) = \sum_{k=1}^{n} A^{k^2}$$, где k – размер матрицы.

Тогда асимптотическая сложность атаки "грубой силы" A^{n^2}.

3.4 Атака на шифровку

Атака на шифр Хилла проведена с использованием средств, которые представлены в Cryptool 1. Атака представлена на рис. 12-16.

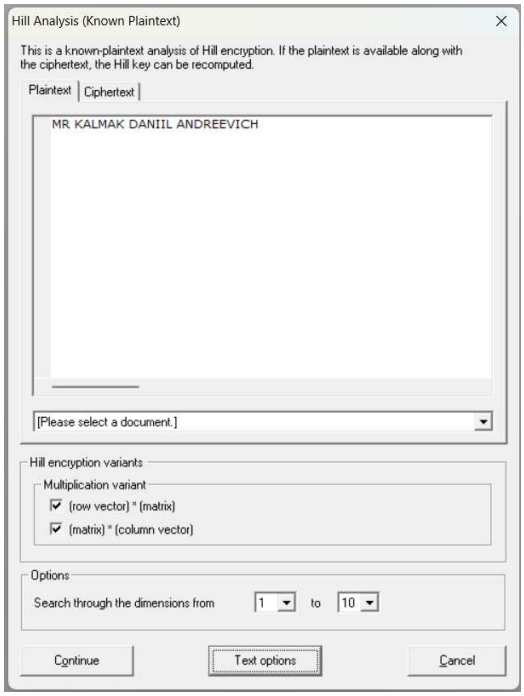

Рисунок 12 – Исходный текст

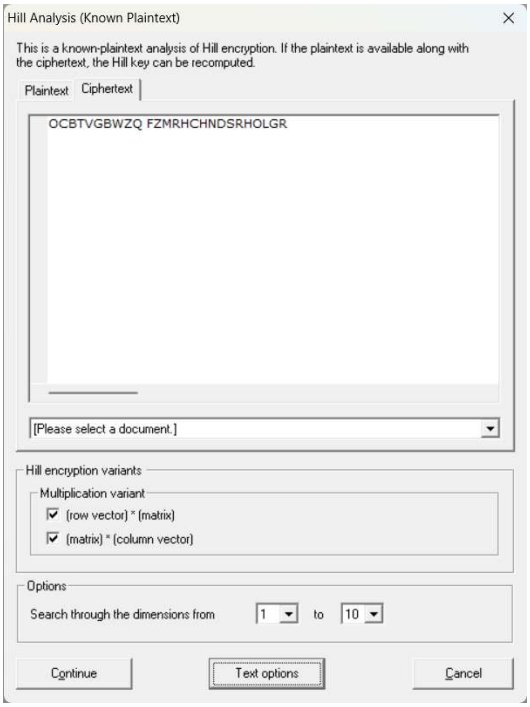

Рисунок 13 – Шифротекст

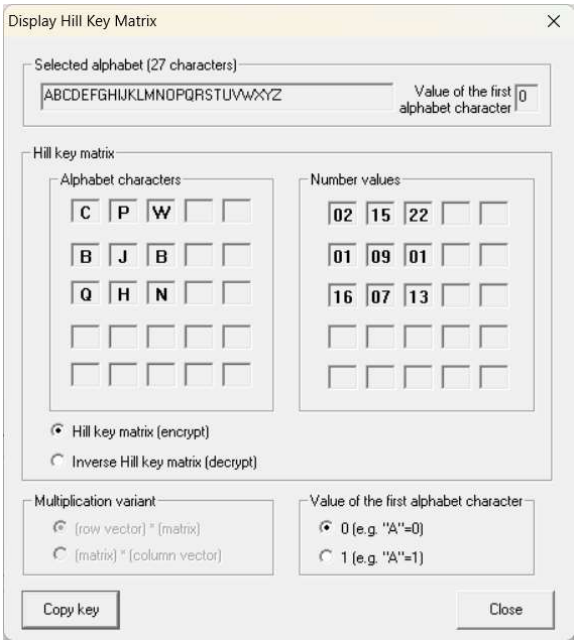

Рисунок 14 - Найденная шифрующая матрица

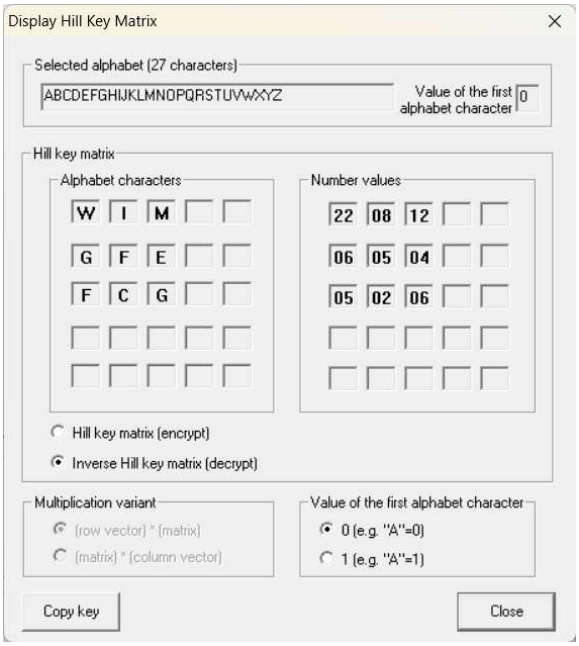

Рисунок 15 – Найденная дешифрующая матрица

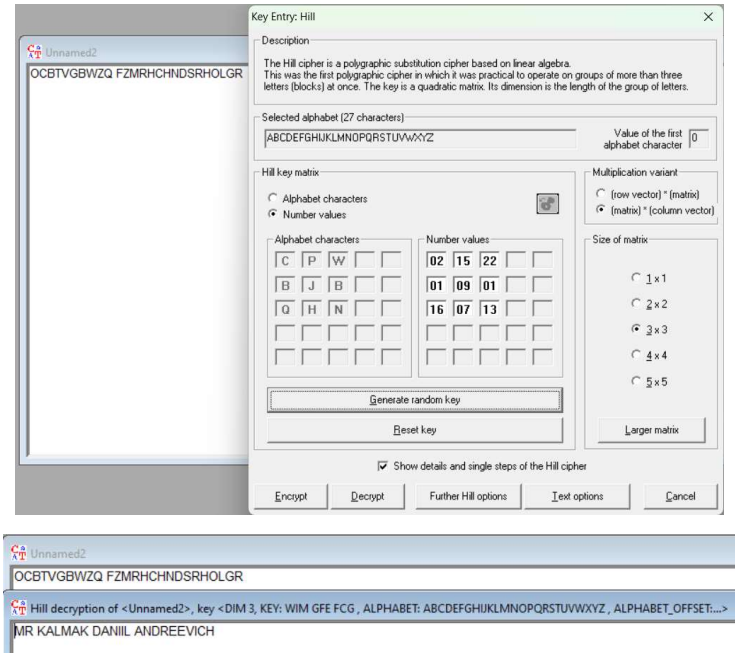

Рисунок 16 – Расшифрованный текст

Выводы.

Таким образом, были исследованы три шифра: шифр «Изгородь» (Rail Fence), шифр Виженера (Vigenere) и шифр Хилла (Hill).

Для шифра «Изгородь» описана схема шифрования и расшифровки. С помощью Cryptool 1 произведено шифрование “0123456789” с высотой изгороди 4 и смещением 2, и получен шифротекст “4359026817”. Проведено расшифрование, в результате которого получен исходный текст, то есть сообщение было успешно расшифровано. Описаны характеристики шифра. Данный шифр перестановочный, ключом являются числа k и m, высота изгороди и сдвиг соответственно, шифр не является блочным. Оценена асимптотическая сложность атаки "грубой силы" n^2. Произведена атака на шифровку LAMKKA с исходным текстом KALMAK с высотой изгороди 3 и смещением 2 с использованием Cryptool 1 и успешно получен исходный текст.

Для шифра Виженера описана схема шифрования и расшифровки. С помощью Cryptool 2 произведено шифрование текста с ключом “SECRETKEY”. Проведено расшифрование, в результате которого получен исходный текст, то есть сообщение было успешно расшифровано. Описаны характеристики шифра. Данный шифр - многоалфавитный шифр замены, ключом является слово, состоящее из символов алфавита, шифр является блочным. Оценена асимптотическая сложность атаки "грубой силы" A^n, где A - длина алфавита, n – длина исходного текста. Произведена атака на шифровку с использованием Cryptool 2 и успешно получен исходный текст за исключением пробелов.

Для шифра Хилла описана схема шифрования и расшифровки. С помощью Cryptool 2 произведено шифрование текста с ключом – шифрующей матрицей $\begin{matrix} 2 & 15 & 22 \\ 1 & 9 & 1 \\ 16 & 7 & 13 \end{matrix}$. Проведено расшифрование, в результате которого получен исходный текст, то есть сообщение было успешно расшифровано. Описаны характеристики шифра. Данный шифр - шифр многоалфавитной замены, но с математическим подходом к шифрованию и дешифрованию.

Матрица исходного текста умножается на ключ, ключом является матрица размером n на n, при этом матрица обратимая, чтобы была возможность расшифровать текст, шифр является блочным. Оценена асимптотическая сложность атаки "грубой силы" A^{n^2}, где A - длина алфавита, n – размер квадратной дешифрующей матрицы. Произведена атака на шифровку с использованием Cryptool 1 и успешно получен исходный текст.