

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

ОТЧЕТ
по лабораторной работе №1
“Изучение классических шифров Caesar, Permutation/Transposition, Hill”
Вариант 8

Студент гр. 8382

Мирончик П.Д.

Преподаватель

Племянников А.К.

Санкт-Петербург

2021

1. ЦЕЛЬ РАБОТЫ

Исследовать шифры Caesar, Permutation/Transposition, Hill и получить практические навыки работы с ними, в том числе с использованием приложений Cryptool 1 и 2.

2. CAESAR

2.1. 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.

2.2. Ход работы

2.2.1. Реализация в CrypTool 1.0

CrypTool предоставляет интерфейс (Рис. 2.1), в котором можно выбрать ключ для шифрования/дешифрования Caesar, указав его либо цифрой, либо буквой; при этом можно отдельно указать, как интерпретировать символы: начиная с 0 или с 1.

Description

Here you can enter the key for the Caesar cipher.

Caesar is a mono-alphabetic substitution, where the characters of the cleartext alphabet are mapped to the ciphertext alphabet by shifting. This shifting value is the key. You can enter the key as a number or as a single character of the alphabet.

Rot-13 is a special variant, where the key has the fixed value of half the length of the cleartext alphabet. This variant is only selectable if the length of the alphabet is an even number.

Select variant

☒ Caesar

☐ Rot-13

Options to interpret the alphabet characters

☒ Value of the first alphabet character = 0 (e.g. "A"=0)

☐ Value of the first alphabet character = 1 (e.g. "A"=1)

Key entry as

☒ Alphabet character

☐ Number value

Properties of the chosen encryption

Shift of 1

Mapping of the alphabet (26 characters)

from:

to:

Рис. 2.1 , интерфейс шифрования CrypTool

Одной из возможностей CrypTool также является построение гистограмм частот для текстов (Рис.2.2).

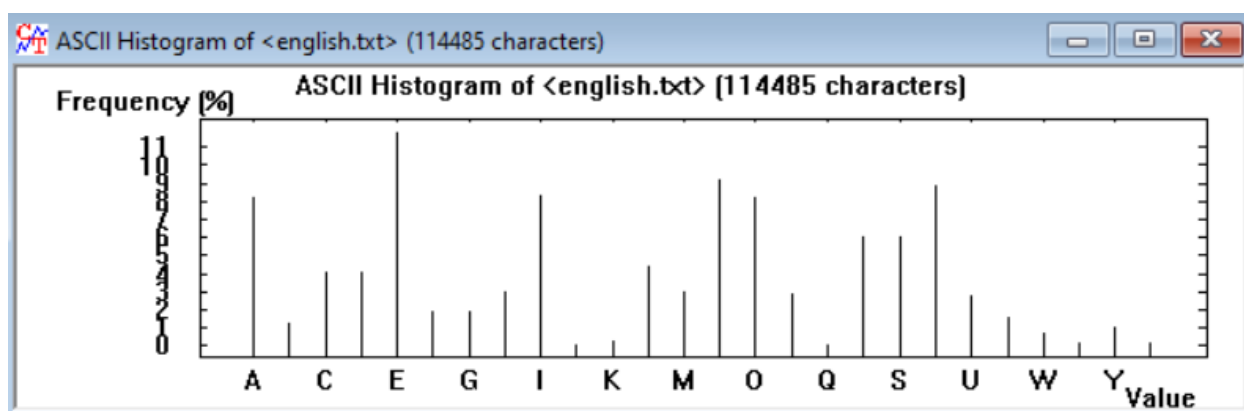


Рис.2.2, гистограмма частот English.txt

2.2.2. Пояснение работы шифра

Суть шифрования в следующем: в одну строку записываются элементы алфавита, выбирается смещение, согласно которому ниже символ под символом записывается используемый нами алфавит, сдвинутый влево на величину смещения. Символ, находящийся под символом исходного алфавита в открытом тексте, является соответствующим символом в шифротексте. На Рис.2.3 представлена таблица для смещения равного 3.

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
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	а	б	в

Рис.2.3, таблица для смещения 3

2.2.3. Пример работы шифра

Зашифруем текст `mironchik` с использованием ключа со сдвигом, равным 1. Полученный результат `njspodijl`, что, очевидно, верно. Символ `m` был заменен на `n`, `i-j`, `r-s` и т.д.

Дешифровка как вручную, так и с использованием CrypTool (с известным ключем), прошла успешно.

2.2.4. Атака на шифротекст

Зашифруем текст файла `CrypTool-en.txt` с использованием ключа со сдвигом 1. Построим для него гистограмму частот (Рис.2.4).

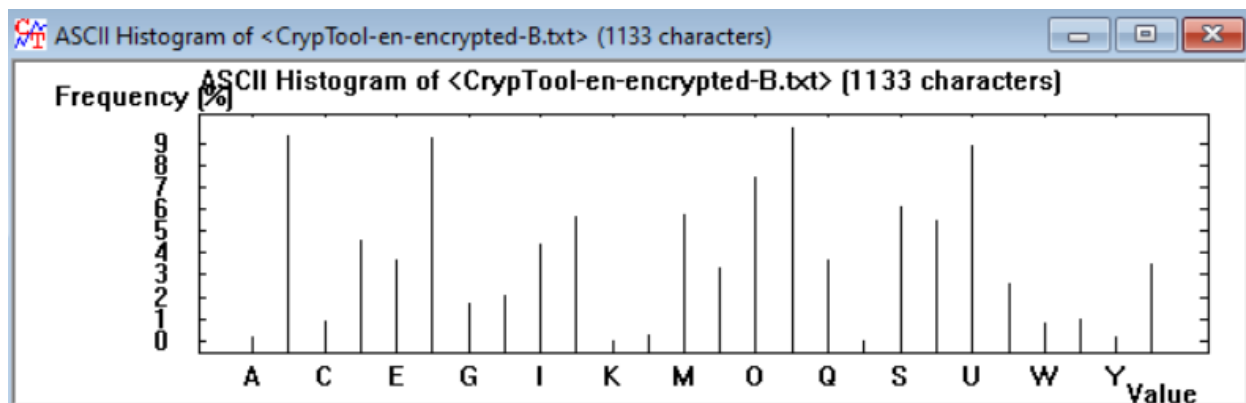


Рис.2.4, гистограмма частот зашифрованного текста

Заметно, что, если сдвинуть полученную гистограмму на один символ влево, она практически совпадет с эталонной (Рис.2.2). В действительности, это не всегда может быть так очевидно, и эффективнее использовать дешифратор CrypTool, который найдет наиболее подходящее смещение с учетом корреляции частот зашифрованного текста и эталонного (Рис.2.5).

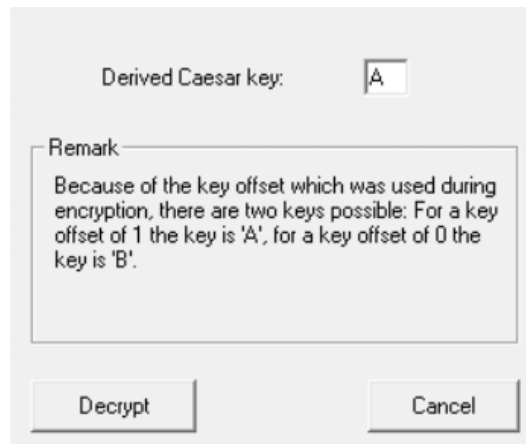


Рис.2.5, ключ, найденный CrypTool

Ключ подошел и текст был успешно декодирован. Стоит отметить, что ключ А на Рис.2.5 соответствует смещению 1.

2.2.5. Оценка шифра

Шифр Цезаря является шифром с заменой, ключем к которому является число $0 \leq n < m$, где m - мощность алфавита. Очевидно, что шифр крайне неустойчив к атакам “грубой силы” и сложность таких атак составляет $O(m)$.

2.3. Заключение

Был изучен шифр Caesar и способы работы с ним в программе CrypTool 1.

В качестве примера был зашифрован текст `mironchik` и для сдвига 1 получен результат `njspodijl`. Определено, что Caesar является шифром с заменой, имеет ключ в виде числа, не превышающего мощность алфавита m , и неустойчив к атакам грубой силы, которые имеют сложность $O(m)$.

Рассмотрен способ атаки на шифротекст с использованием гистограмм распределения частот на тексте файла `CrypTool-en.txt`, изучен инструмент проведения автоматической атаки, реализованный в CrypTool 1. В результате проведения пробной атаки текст был успешно дешифрован и получен верный исходный текст.

3. PERMUTATION/TRANSPOSITION

3.1. 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.

3.2. Ход работы

3.2.1. Реализация в CrypTool 1

CrypTool 1 предоставляет интерфейс, содержащий две перестановки, которые имеют одинаковые настроечные параметры и настраиваются отдельно. Рассмотрим параметры перестановки (Рис. 3.1).

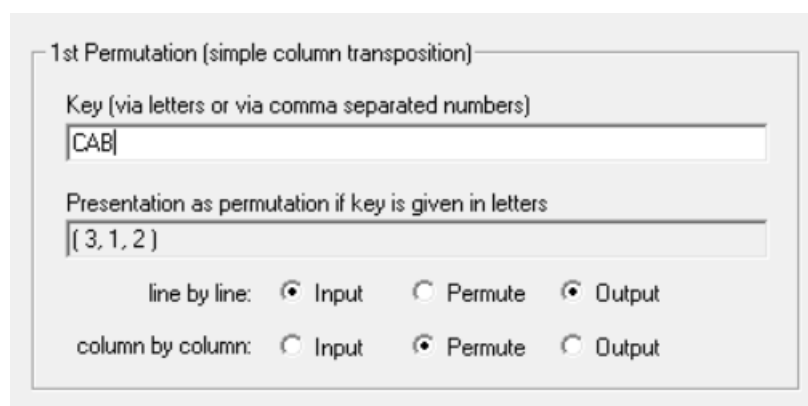


Рис.3.1. Параметры перестановки Permutation/Transposition в CrypTool 1

В поле key предлагается ввести ключ, состоящий из чисел или букв. Буквы транслируются в числа следующим образом: каждой букве ставится в соответствие число, равное $n + m$, где n - количество букв в ключе, имеющих меньший порядковый номер в алфавите, а m - количество букв, имеющих такой же порядковый номер в алфавите, и имеющих меньший порядковый номер в ключе.

Полученный набор является номерами столбцов (или строк, в зависимости от настройки Permute), которые будут отсортированы по возрастанию. Например, для текста ABC и ключа 3, 1, 2, закодированный вариант будет BCA.

Настройка Permute позволяет указать, чем является ключ: номерами строк, или номерами столбцов. Так в случае, если Permute выбран для line by line, ключ будет соответствовать номерам строк (т.е. если n - количество чисел в ключе, то матрица будет содержать n строк, и перестановка будет осуществляться по строкам).

Настройка Input указывает, как должно производиться заполнение данных: по строкам или по столбцам. Приведем пример для текста ABCDEF и ключа 3,1,2 (т.е. матрица состоит из трех строк). При заполнении построчно будет получена матрица, указанная в табл.3.1, при заполнении по столбцам - матрица, указанная в табл.3.2.

<i>3</i>	<i>A</i>	<i>B</i>
<i>1</i>	<i>C</i>	<i>D</i>
<i>2</i>	<i>E</i>	<i>F</i>

Табл.3.1. Построчное заполнение

<i>3</i>	<i>A</i>	<i>D</i>
<i>1</i>	<i>B</i>	<i>E</i>
<i>2</i>	<i>C</i>	<i>F</i>

Табл.3.2. Заполнение по столбцам

Наконец, настройка Output указывает, как будет прочитана таблица со сдвинутыми столбцами или строками: по строкам (первая опция) или по столбцам (вторая опция).

После выполнения первой перестановки полученный текст передается во вторую перестановку, которая выполняется аналогично первой.

С учетом задания к лабораторной работе, параметры Input и Output всегда будут находиться в положении line by line, а Permute будет меняться в зависимости от того, переставляем мы строки или столбцы.

2.2.6. Пример работы шифра

Условимся, что ключ состоит из двух последовательностей чисел, первая характеризует перестановки по строкам, вторая - по столбцам.

Пусть шифруемый текст MironchikPavelDenisovich, ключ - (1,4,3,2)(4,1,2,5,6,3). Зашифрованный текст - ircMonovhsiclDieenikvhPa, что, очевидно, аналогично шифрованию вручную (Табл.3.3).

	4	1	2	5	6	3
1	<i>M</i>	<i>I</i>	<i>r</i>	<i>o</i>	<i>n</i>	<i>c</i>
4	<i>h</i>	<i>I</i>	<i>k</i>	<i>P</i>	<i>a</i>	<i>v</i>
3	<i>e</i>	<i>l</i>	<i>D</i>	<i>e</i>	<i>n</i>	<i>i</i>
2	<i>s</i>	<i>o</i>	<i>v</i>	<i>I</i>	<i>c</i>	<i>h</i>

Табл.3.3. Шифрование вручную

2.2.7. Характеристики шифра

Шифр Permutation/Transposition является шифром с перестановкой. Если известно, что шифруемый текст построчно заполняет матрицу (возможно, оставляя незаполненными последние ячейки последней строки), то ключом к шифру является перестановка столбцов, строк и очередность выполнения перестановок.

Очевидно, что, при известном количестве строк и столбцов матрицы, сложность атаки “грубой силы” составляет $n! * m!$, где n, m - количество строк и столбцов матрицы.

2.2.8. Атака с использованием средств CrypTool 1

CrypTool 1 предлагает дешифровку с использованием известных исходного и зашифрованного текстов и с условием, что была выполнена одинарная перестановка. Для этого, помимо текстов, предлагается ввести также параметры перестановки: Input, Permuted, Output и границы количества переставляемых столбцов (или строк). Их указание необходимо для того, чтобы сузить количество ключей, которые будут перебираться в поисках подходящего. Также необходимо учитывать, что возможен вариант, когда подойдут одновременно несколько ключей.

Приведем пример атаки на одиночную перестановку. Исходный текст MironchikPavelDenisovich, ключ - (2,1,4,3) (перестановка выполняется по строкам). Зашифрованный текст - hikPavMironcsovichelDeni. Указываем следующие параметры в анализаторе CrypTool 1 (Рис.3.2).

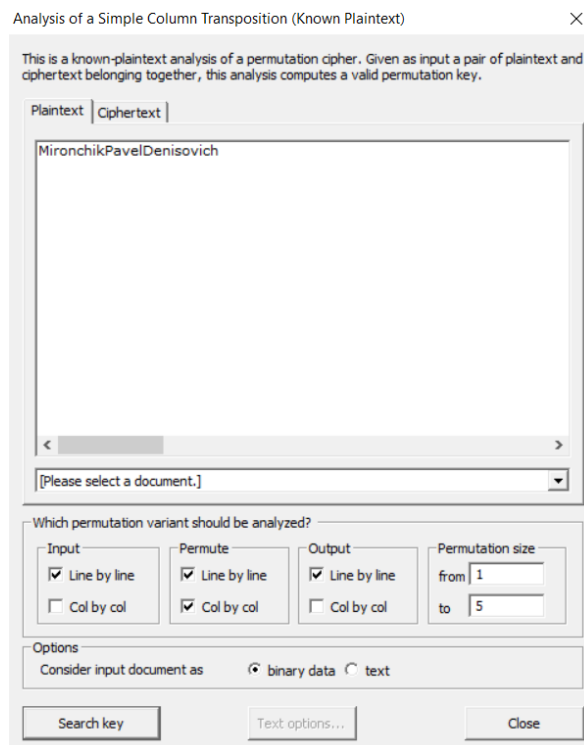


Рис.3.2. Параметры для дешифровки сообщения CrypTool 1

В результате дешифратор обнаружил один подходящий под заданные требования ключ (Рис.3.3), действительно соответствующий указанному при шифровке.

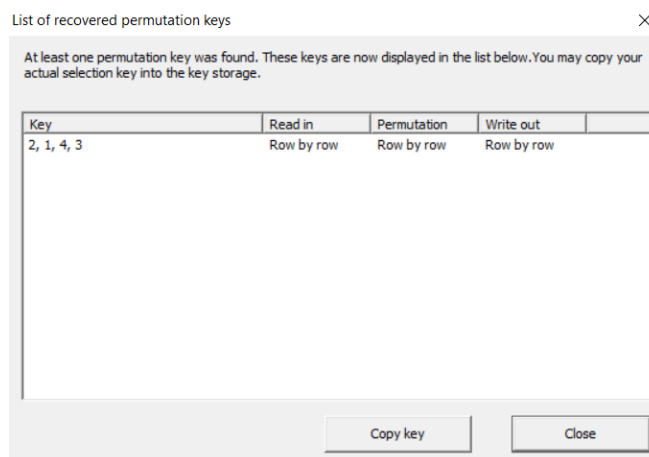


Рис.3.3. Результат дешифровки средствами CrypTool 1

2.2.9. Атака коллеги

Было зашифровано сообщение DEAR colleague TNAHKS с использованием одинарной перестановки по столбцам (3,4,1,2). Зашифрованное сообщение выглядит как ARDEol cagle TueHKNAS. Коллега успешно расшифровал сообщение и получил DEAR colleague TNAHKS.

2.2.10. Атака на шифр в CrypTool 2

CrypTool 2 предлагает несколько вариантов атак на шифр перестановки.

1. Алгоритм “грубой силы”. Перебор всех возможных вариантов ключей с присвоением оценки каждому ключу.

2. Crib Analysis. Для работы алгоритма необходим фрагмент исходного текста, который позволяет сузить количество возможных ключей.

3. Генетический алгоритм. Генерируется набор случайных ключей, который обрабатывается следующим алгоритмом:

1. Из списка ключей выбирается лучшая половина, худшая половина отбрасывается.

2. Далее из оставшихся ключей генерируются новые пары, которые определенным образом видоизменяются и добавляются к набору.

3. Переход к первому шагу.

Алгоритм повторяется, пока не будет превышено максимальное количество итераций.

4. Алгоритм восхождения (Hillclimbing Algorithm). Генерируется и оценивается случайный ключ. Далее в ключ вносятся небольшие изменения и полученный ключ сравнивается с исходным. Если новый ключ имеет большую “стоимость”, он принимается и становится исходным, в противном случае новый ключ отбрасывается. Как и генетический алгоритм, процедура повторяется определенное количество раз.

3.3. Заключение

В ходе выполнения работы был рассмотрен шифр Permutation/Transposition.

Определено, что шифр Permutation/Transposition является шифром с перестановкой. Ключем к шифру является перестановка столбцов, перестановка строк и очередность выполнения перестановок, а сложность атаки “грубой силы” составляет $O(n! * m!)$, где n, m - количество строк и столбцов матрицы. Рассмотрены инструменты работы с шифром в программе CrypTool 1: шифрование/дешифрование, поиск ключа с учетом известного исходного текста. Также через официальные документ помощи рассмотрены способы атаки на шифр средствами CrypTool 2: алгоритм грубой силы, Crib Analysis, генетический алгоритм и алгоритм восхождения.

Коллегой была проведена успешная атака на текст *DEAR colleague THANKS*, зашифрованный одинарной перестановкой по столбцам (3,4,1,2), при том, что коллеге были известны префикс и постфикс шифруемого текста, а также то, что перестановка была одинарной.

4. HILL

4.1. 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.

4.2. Ход работы

4.2.1. Описание шифра

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 (Рис.4.1). Для расшифровки необходимо шифротекст

умножить на матрицу, которая является мультипликативной инверсией по отношению к шифрующей для выбранного алфавита (Рис.4.2).

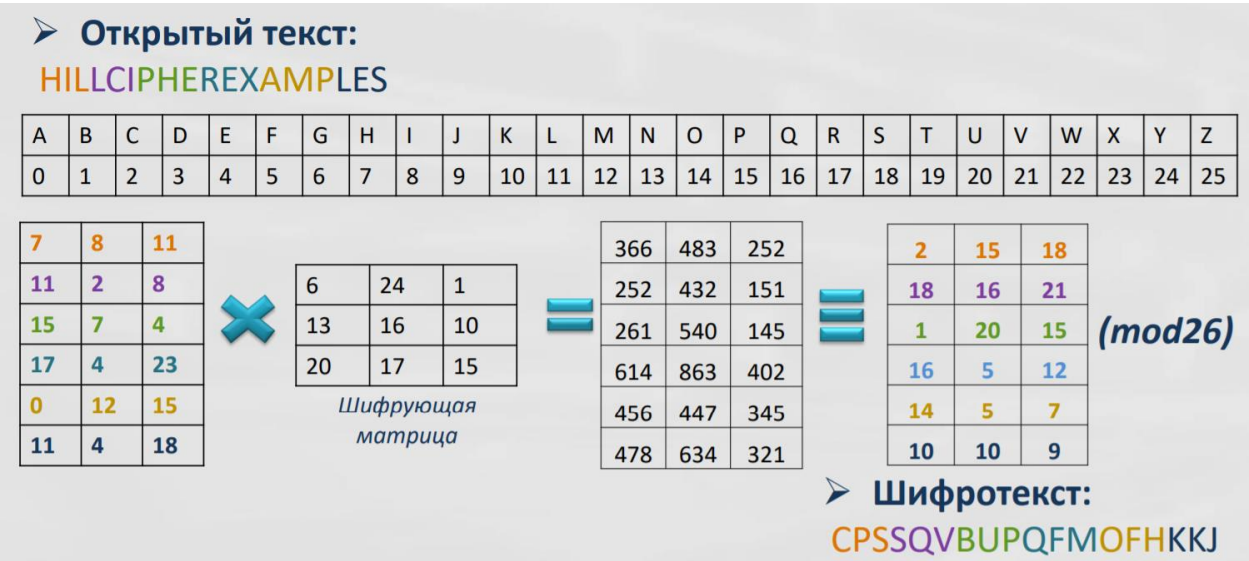


Рис. 4.1, пример зашифрования



Рис.4.2, пример расшифрования

4.2.2. Реализация в CrypTool 1

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)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Value of the first alphabet character

Hill key matrix

☒ Alphabet characters 
☐ Number values

Alphabet characters

Number values

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

Рис.4.3, интерфейс шифра Hill в CrypTool 1

CrypTool 1 позволяет проводить зашифрование и расшифрование, требуя на вход только исходный/зашифрованный текст, ключ зашифрования и список символов исходного алфавита (Рис.4.3). Список символов исходного алфавита при этом задается в отдельном окне (Рис. 4.4), что позволяет избежать возможной путаницы в сравнении со случаем, когда список символов задавался бы вручную текстом.

The image shows a settings window for CryptTool 1. It is divided into four main sections:

- Formatting options for cleartext and ciphertext:** Contains a checked checkbox labeled "Keep characters not present in the alphabet unchanged".
- Upper/lower case in cleartext and ciphertext:** Contains two checkboxes: "If possible, retain case information for encryption/decryption" (checked) and "Distinguish between uppercase and lowercase" (unchecked).
- Define the alphabet used in text ciphers:** Contains six checkboxes: "Uppercase letters" (checked), "Lowercase letters" (unchecked), "Space" (unchecked), "Special characters" (unchecked), "Numerals" (unchecked), and "Umlauts" (unchecked). Below these is a text field labeled "Alphabet to use (26 characters):" containing the string "ABCDEFGHIJKLMNOPQRSTUVWXYZ".
- Reference file for statistical applications:** Contains a text field with the path "F:\ProgramFiles\CrypTool\reference\english.txt" and a "Find..." button. Below this is a dropdown menu currently showing "English reference file".

At the bottom of the window are three buttons: "Apply", "Restore default", and "Cancel".

Рис.4.4, задание списка символов исходного алфавита

Также в CrypTool 1 присутствует алгоритм дешифрования на основе знания исходного текста, представленный на рис.4.5.

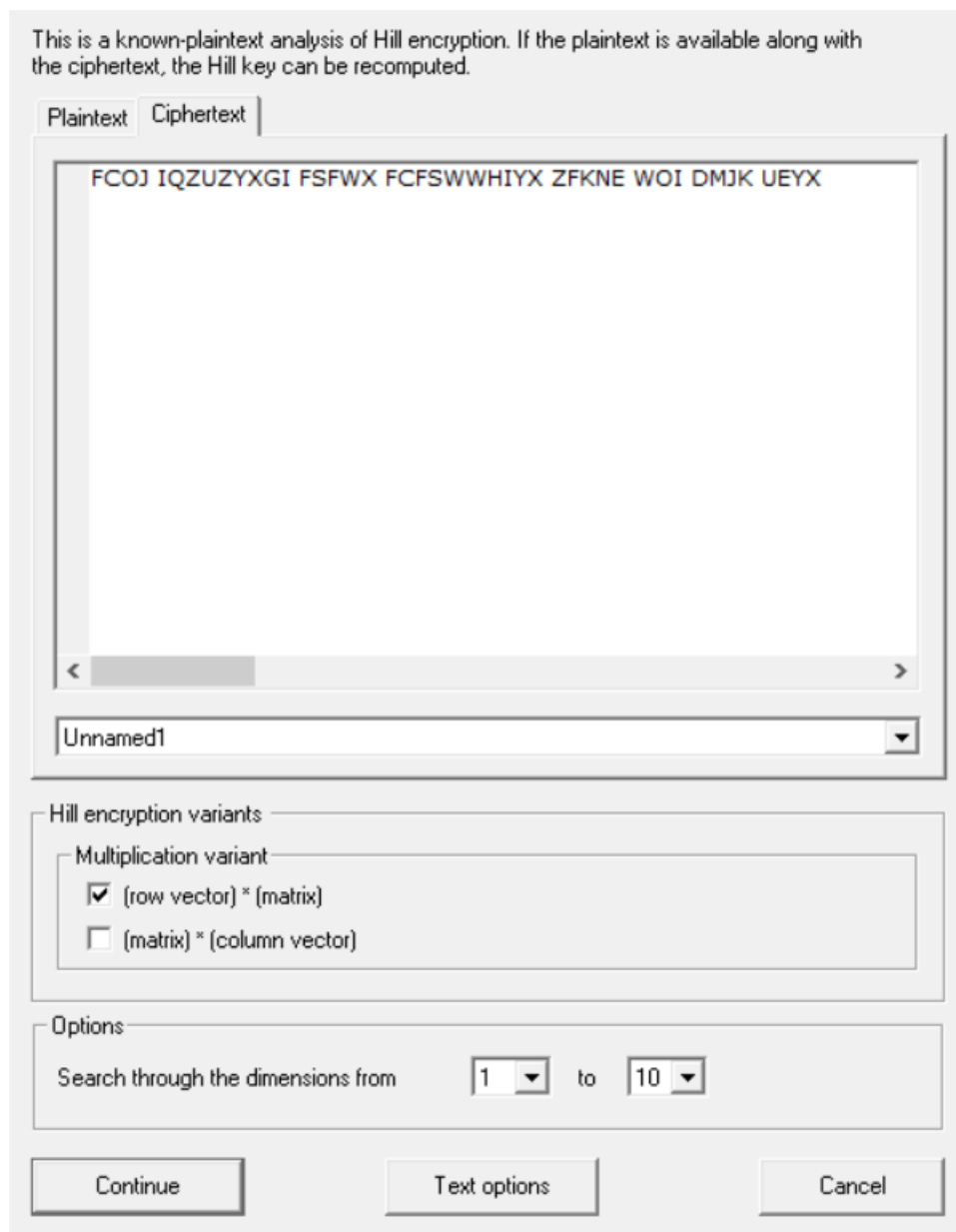


Рис.4.5, дешифрование на основе знания исходного текста

4.2.3. Пример работы шифра

Зашифруем текст *DEAR MIRONCHIK PAVEL DENISOVICH THANK YOU VERY MUCH* с использованием ключа - матрицы размером 3×3 :

14	5	17
5	17	19
21	24	25

Получим зашифрованный текст *TTUB NESMVAJLQ HPQGX GGHHCNFNHYJ LPKJH BYF OQRR QJCZR*.

4.2.4. Характеристики шифра

Шифр Хилла является симметричным блочным шифром с заменой, ключом к которому является матрица $m \times m$.

Сложность атаки “грубой силы” на шифр составляет в худшем случае $n^{m \times m}$ – количество всех возможных матриц размера $m \times m$.

4.2.5. Атака с использованием CrypTool 1

CrypTool 1 предоставляет интерфейс для реализации атаки на основе известного исходного текста (Рис.4.5). Проведем атаку на примере сообщения из пункта 4.2.3. Полученный ключ:

14	5	17
5	17	19
21	24	25

Ключ совпал с ключом зашифрования, использованным в пункте 4.2.3.

Зашифруем теперь текст *DEAR THANK YOU VERY MUCH*: получим *TTUT JRKJH BYF OQRR QJCZR*. Заметно, что начальные и конечные зашифрованной части сообщений совпали с пункта 4.2.3, что объясняется тем, что удаленная часть сообщения кратна размеру шифрующей матрицы. При проведении атаки на этот текст был получен тот же самый ключ, т.к. количество строк в шифруемой матрице превышает размер матрицы шифрования и ключ можно восстановить однозначно.

4.2.6. Атака коллеги

Атака проводилась на шифровку из пункта 4.2.3. Очевидно, что, если известны начальные и конечные части сообщений, из них можно вырезать среднюю, неизвестную часть, и работать с оставшейся как с известным текстом. Таким образом, исследовав предположения о размере ключа 2×2 и 3×3 был найден ключ зашифрования и с его использованием дешифрован зашифрованный текст:

14	5	17
5	17	19
21	24	25

4.3. Заключение

В ходе выполнения работы был исследован шифр Хилла.

Определено, что этот шифр является симметричным блочным шифром с заменой, сложность атаки грубой силы на который составляет n^{m*m} в худшем случае.

В работы описано использование шифра средствами CrypTool 1 на примере зашифрования и расшифрования текста *DEAR MIRONCHIK PAVEL DENISOVICH THANK YOU VERY MUCH* и ключа-матрицы размером 3×3 .

Далее была проведена атака на шифр на основе известного исходного текста средствами CrypTool 1 и восстановлен верный ключ зашифрования.

После этого из исходного и зашифрованного текстов была удалена часть, содержащая *MIRONCHIK PAVEL DENISOVICH*, и проведена повторная зашифровка и расшифровка, в результате которой успешно был получен ключ шифрования.

В конце была проведена атака коллеги по тем же принципам: удаление средней, неизвестной части и использование оставшихся частей в качестве текста. В результате атаки так же был успешно получен исходный ключ шифрования.