

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

**ЛАБОРАТОРНАЯ РАБОТА №3
по дисциплине «Криптография и защита информации»
Тема: Изучение классических шифров Hill, ADFGVX, Playfair**

Студент гр. 6304

Преподаватель

Корытов П.В.

Племянников А.К.

Санкт-Петербург

2019

Цель работы

Цель работы: исследовать шифры Hill, ADFGVX, Playfair и получить практические навыки работы с ними, в том числе и в программном продукте CrypTool 1 и 2.

1. Шифр Хилла

1.1. Описание шифра

Зашифровка шифром Хилла:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Текст — HILLCIPHEREXAMPLES

$$\begin{pmatrix} 7 & 8 & 11 \\ 11 & 2 & 8 \\ 15 & 7 & 4 \\ 17 & 4 & 23 \\ 0 & 12 & 15 \\ 11 & 4 & 18 \end{pmatrix} \times \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} = \begin{pmatrix} 366 & 483 & 522 \\ 252 & 432 & 151 \\ 261 & 540 & 145 \\ 614 & 863 & 402 \\ 456 & 447 & 345 \\ 478 & 634 & 321 \end{pmatrix} \equiv \begin{pmatrix} 2 & 15 & 18 \\ 18 & 16 & 21 \\ 1 & 20 & 15 \\ 16 & 5 & 12 \\ 14 & 5 & 7 \\ 10 & 10 & 9 \end{pmatrix} \pmod{26}$$

Шифрующая матрица

Шифротекст: CPSSQVBUPQFMOFHKKJ

Требования к шифрующей матрице — она должна быть обратима, т.е. $|M| \neq 0$. В таком случае M^{-1} — мультипликативная инверсия в \mathbb{Z}_{26} : $M \times M^{-1} \equiv I \pmod{26}$

Расшифровка:

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

Обратная матрица

1.2. Формулировка задания

1. Найти шифр в СrypTool 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. Передайте произвольную шифровку коллеге для расшифрования при условии, что формы обращения и завершения сообщения известны. Размер использованного ключа держать в секрете.

1.3. Ход работы

1. Найден шифр в СrypTool1. Параметры шифра на рисунке 1
2. Фамилия автора — KORYTOV

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$|A| = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 1 * 4 - 3 * 2 = -2$$

Матрица шифрования обратима

$$\begin{pmatrix} 10 & 14 \\ 17 & 24 \\ 19 & 14 \\ 21 & 0 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 62 & 86 \\ 106 & 147 \\ 80 & 113 \\ 42 & 63 \end{pmatrix} = \begin{pmatrix} 10 & 8 \\ 2 & 17 \\ 2 & 19 \\ 16 & 11 \end{pmatrix} \pmod{26}$$

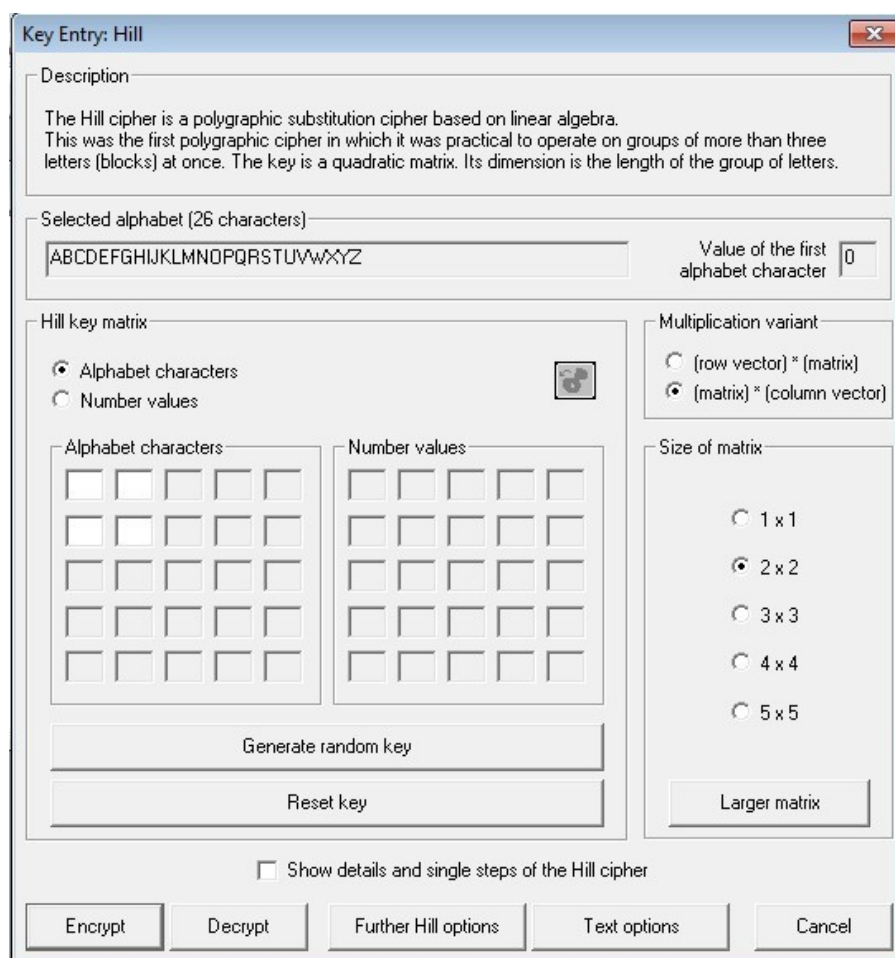


Рисунок 1. Параметры шифра Хилла

Шифротекст — KICRCTQL

Расшифровка:

$$A^{-1} = \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix}$$

$$\begin{pmatrix} 10 & 8 \\ 2 & 17 \\ 2 & 19 \\ 16 & 11 \end{pmatrix} \times \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} -16 & 14 \\ 43 & -28 \\ 19 & -12 \\ -31 & 26 \end{pmatrix} = \begin{pmatrix} 10 & 14 \\ 17 & 24 \\ 19 & 14 \\ 21 & 0 \end{pmatrix}$$

Результаты совпадают

3. Зашифрован текст: DEAR MR KORYTOV PAVEL VALERIEVICH THANK YOU VERY MUCH с ключом JBN WXI JWW.

Результат: HCLQ GL ZCSVLGA BZOSZ KEPXXOBLYOT SMYLO AQJ TCTI JLWO

4. Проведена атака на основе открытого текста текста. Результаты на
5. Из сообщения удалено ФИО автора. Дешифрованный ключ совпадает с исходным

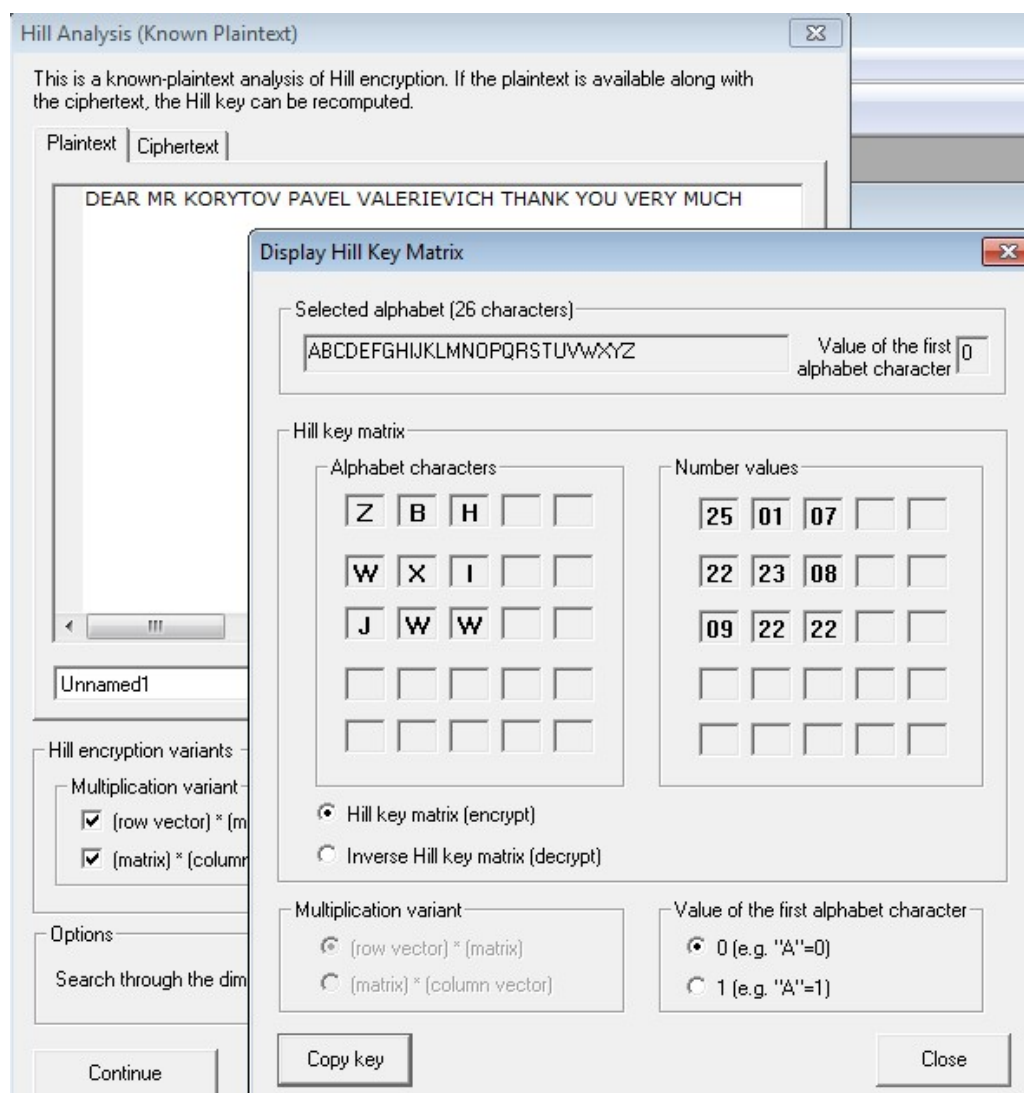


Рисунок 2. Атака на шифр основе открытого текста

6. Коллеге для дешифрования передано следующее сообщение: LADIES AND GENTELMEN YOU HAVE WRONG UNDERSTANDING OF REASON AND THEREFORE THINK YOU EXIST FOR NO REASON THANK YOU. Ключ — YJ PU. Шифротекст: XEHSCK IXN CEJDINWEJ UMG JKJQ QBEDG OFTMPKPCZVAVM KR FEWAUV KZV HTSPCXITM FDERM UMC YNAYV NUR JI TEWAUD TBSRM UMEX

7. Дешифрование полученного текста:

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc.

Display Hill Key Matrix

Selected alphabet (26 characters)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Value of the first alphabet character 0

Hill key matrix

Alphabet characters

Z	B	H		
W	X	I		
J	W	W		

Number values

25	01	07		
22	23	08		
09	22	22		

☒ Hill key matrix (encrypt)

☐ Inverse Hill key matrix (decrypt)

Multiplication variant

☒ (row vector) * (matrix)

☐ [matrix] * (column vector)

Value of the first alphabet character

☒ 0 (e.g. "A"=0)

☐ 1 (e.g. "A"=1)

Copy key

Close

Рисунок 3. Повторение атаки на основе открытого текста

Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

2. Комбинированный шифр ADFGVX

Шифрование осуществляется в два этапа. На первом этапе задается матрица, заполненная символами алфавита, а также цифрами от 0 до 9. Далее каждый символ кодируется парой символов, на пересечении которых он находится. На втором этапе производится перестановка столбцов, заданная кодовым словом.



Рисунок 4. Первый шаг зашифровки

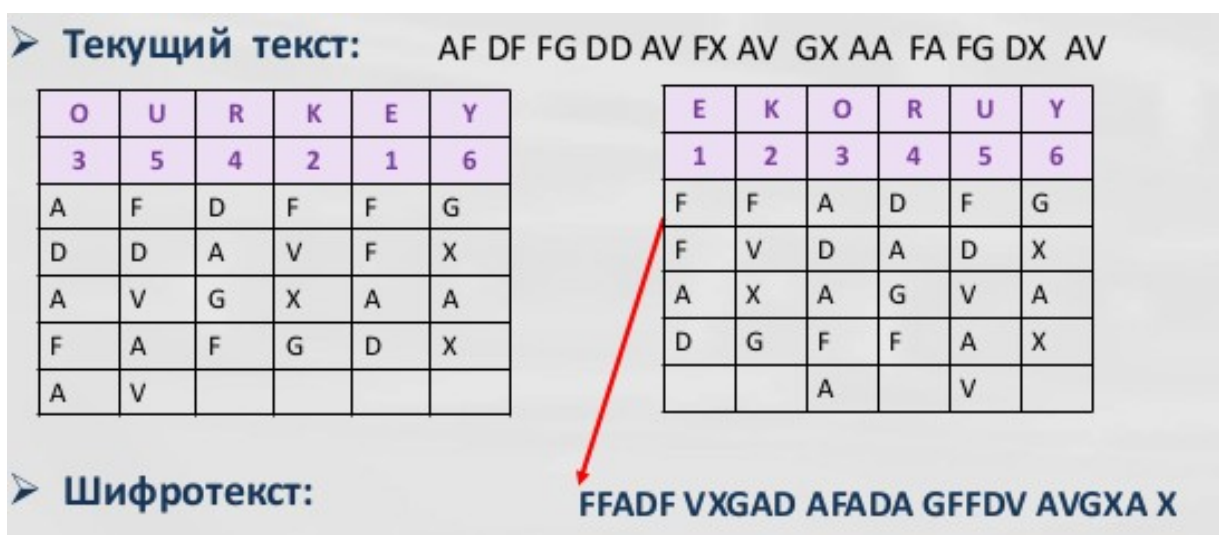


Рисунок 5. Второй шаг зашифровки

2.1. Формулировка задания

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. Выбрать абзац (примерно 600 символов) из файла English.txt (папка CrypTool / reference) и зашифровать его.
4. Выполнить атаку на шифротекст, используя приложение из Analysis-> Symmetric Encryption (classic)-> Cipher Text Only.
5. Повторить шифрование и атаку для тестов примерно в 300 и в 150 символов.

6. Изучите ручное расшифрование для текстов менее 300 символов.
7. Зашифруйте текст из 200 символов, сохраните ключ, и передайте соседу для расшифровки.
8. Самостоятельно изучите атаку по словарю, реализованную в CrypTool 2, опираясь на Help и ссылки на статьи.

2.2. Ход работы

1. Найден шифр в CrypTool 1. Для использования шифра пришлось делать размер окна VirtualBox выше, чем размер экрана. Параметры шифра на рисунке 6
2. Фамилия автора — KORYTOV, выбранный ключ: PAVEL

	A	D	V	G	F	X
A	A	B	C	D	E	F
D	G	H	I	J	K	L
V	M	N	O	P	Q	R
G	S	T	U	V	W	X
F	Y	Z	0	1	2	3
X	4	5	6	7	8	9

Результаты первого шага зашифровки: DF VV VX FA GD VV GG

P	A	V	E	L	A	E	L	P	V
4	1	5	2	3	1	2	3	4	5
D	F	V	V	V	F	V	V	D	V
X	F	A	G	D	F	G	D	X	A
V	V	G	G		V	G		V	G

Шифротекст: FFVVG GVDDX VVAG.

Поскольку длина ключа — 5, а длина шифротекста — 14, в столбце с буквой, обратной последней букве ключа (V) будет на один символ меньше.

Результат первого шага расшифровки: DF VV VX FA GD VV GG

Второй шаг дает исходный текст: KORYTOV

P	A	V	E	L
4	1	5	2	3
<i>l</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
1	2	3	4	5
<i>2</i>	<i>4</i>	<i>5</i>	<i>l</i>	<i>3</i>
<i>E</i>	<i>P</i>	<i>V</i>	<i>A</i>	<i>L</i>

E	P	V	A	L
<i>2</i>	<i>4</i>	<i>5</i>	<i>l</i>	<i>3</i>
F	V	V	D	V
F	G	D	X	A
V	G		V	G

A	E	L	P	V
<i>l</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
D	F	V	V	V
X	F	A	G	D
V	V	G	G	

Key Entry: ADFGVX

Step 1: Substitution

Substitution matrix

	A	D	F	G	V	X
A	A	B	C	D	E	F
D	G	H	I	J	K	L
F	M	N	O	P	Q	R
G	S	T	U	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

The substitution matrix replaces each plaintext letter by a pair of the letters A,D,F,G,V,X.

The matrix must contain each letter A-Z and each cipher 0-9 exactly once.

Standard matrix

Random matrix

Erase matrix

Enter string

Step 2: Transposition

The encryption only uses the characters of the transposition password that are part of the current alphabet (see text options).

Transposition password

Column sequence

Text options

Output options

Result: Ciphertext after step 2

☐ Separate output blocks by blanks
 Block length (1-26):

☐ New line after each block

Intermediate result: Ciphertext after step 1

☐ Print out intermediate result

☒ Separate output blocks by blanks
 Block length (1-26):

☐ New line after each block

Encrypt

Decrypt

Cancel

Рисунок 6. Параметры шифра ADFGVX

9

3. Выбран абзац из Agenda 21 длиной в 600 символов и зашифрован. Результат на

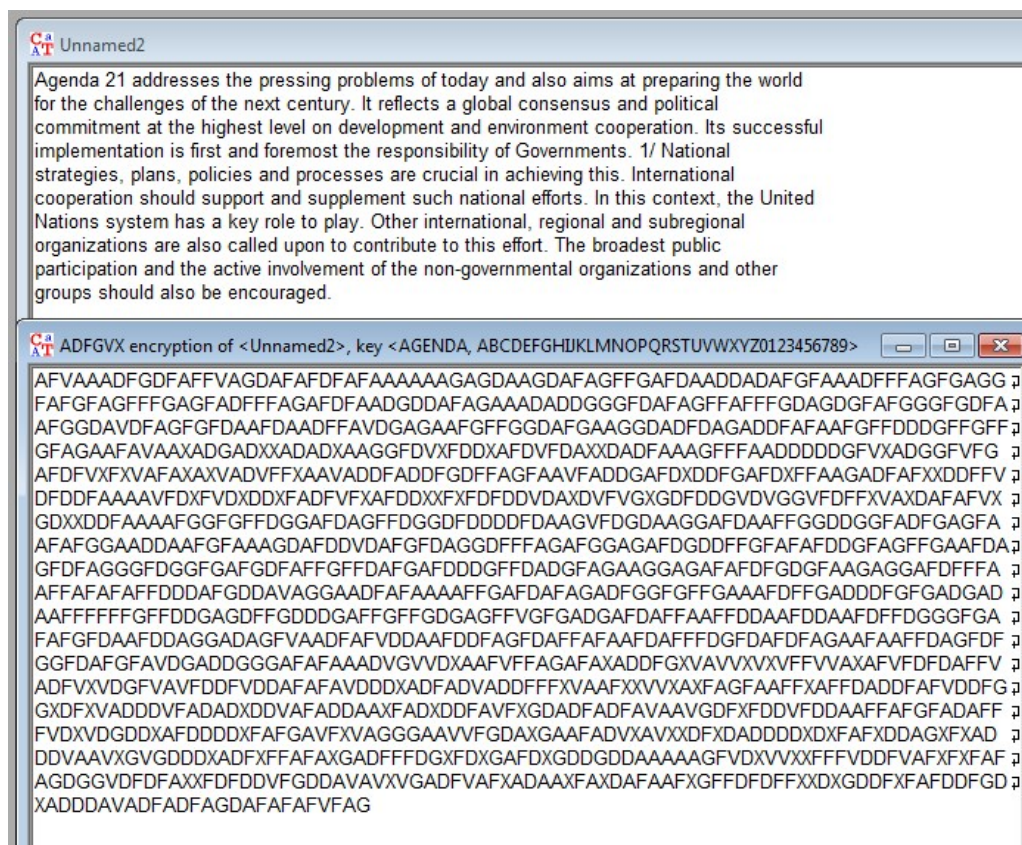


Рисунок 7. Зашифровка абзаца Agenda 21

4. Выполнена атака на шифротекст. Атака выполнена успешно; однако, для получения результата пришлось возвращать матрицу подстановки в стандартный вид. Результаты на рисунке 8
5. Текст длиной в 300 символов дешифрован успешно, но количество итераций дешифровки составило 9. Для текста длиной в 150 символов число итераций приблизилось к 100.
6. Ручное дешифрование для текстов менее 300 символов — трудоемкая задача, особенно без вычислительного оборудования. Жорж Пенвен, взломавший шифр в 1918 году, использовал для дешифрования сообщения со стандартным началом; по повторяющимся фрагментам шифротекста определялась вероятная длина ключа.
- Кроме того, можно определить, какие буквы составляют столбцы, а какие — строки, т.к. между этапами зашифровки они чередуются. Объединение четных и нечетных пар и их частотный анализ позволяли определить, являются ли они результатом замены символов открытого текста.

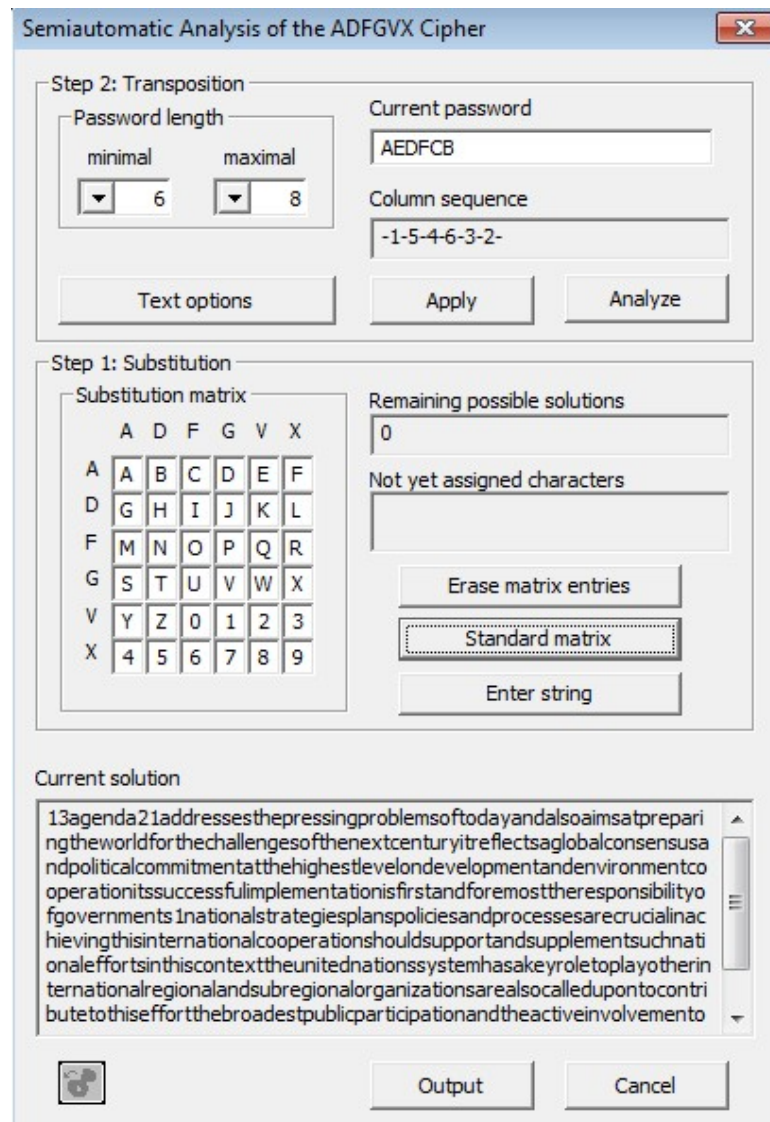


Рисунок 8. Атака на шифр ADFGVX

Таким образом, требуется объемный статистический анализ, который сложно провести вручную; для недостаточного объема текста это практически невозможно.

7. Ключом “HUMAN” зашифрована следующая цитата Чарльза Дарвина: “When I view all beings not as special creations, but as the lineal descendants of some few beings which lived long before the first bed of the Cambrian system was deposited, they seem to me to become ennobled”

Результат шифрования: “DDFAX DAFAF FDXGF ADGVF AAFAD FAAVA DGFDG DDAFG VFDAX AAFAV DGAFAD VVVG AFVVFV FXGVG VDDFA GAAFA VDDGA DXAXG VADAF AVDAD FDFVA AXDXG DFDAAD DDGVA GFFAD GVFVA FADAV DDDVD VDDAA AAFAF AGAAF AGADF AGAAD FADDG GFDFV AFGVA DADAA GAGVG DGVAAD FADFA DDGAF AAAFG FGGDX ADFDA DDDDV AGGFF VGVDV AXAXD VFDAX AGGVF XFAAV

AGDVD AADAF AAFFA VFGGX ADFDG VAFAF GFGDD VAAFA GXFXA
FGDDF AFAXA DDAAF DFAFG AFAAF GGAAF FGDFV FDA”

Сообщение передано коллеге для расшифровки.

8. Дешифрование полученного текста

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

3. Шифр Плейфера (Playfair)

3.1. Описание шифра

Исходный текст разбивается на блоки — биграммы по 2 символа. Ключом является матрица 5×5 . 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

3.2. Формулировка задания

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 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. Передайте произвольную шифровку соседу для расшифрования при условии, что форма обращения, используемая в сообщении, известна. Размер использованной матрицы (ключа) держать в секрете.

3.3. Ход работы

1. Найден шифр в Cryptool 1. Параметры шифра на рисунке 9
2. Для ручного зашифрования выбрана следующая матрица-ключ:

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

Зашифрование: KORYTOV \Rightarrow KO RY TO V \Rightarrow KO RY TO VX \Rightarrow OP BU CX XY

Расшифрование: OP BU CX XY \Rightarrow KO RY TO VX \Rightarrow KORYTOV

Key Entry: Playfair

Options

☒ Separate duplicate letters

First separator: X

Second separator: Y

☒ Separate duplicate letters only within pairs

☒ Ignore duplicate letters in the key phrase

Playfair key

Short version of the Playfair key:

Key matrix

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

☒ 5x5 matrix

☐ 6x6 matrix

Encrypt Decrypt Cancel

Рисунок 9. Параметры шифра Playfair

3. Зашифрован следующий текст: DEAR ALL THANK YOU FOR NOT BEING HERE AND IF YOU ARE HERE PLEASE LEAVE с ключом LEAVEMEBEHIND. Результаты на рисунке 10

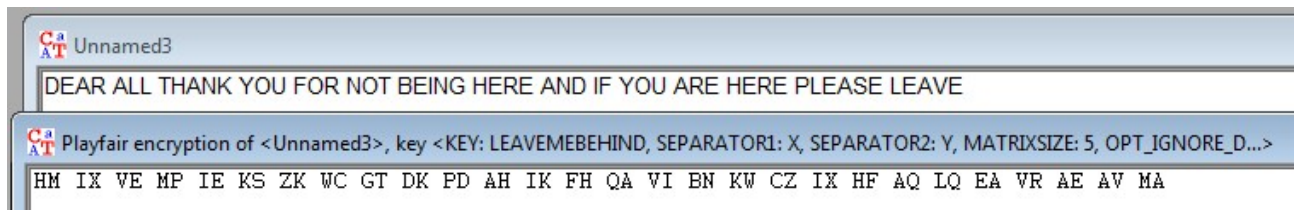


Рисунок 10. Результаты шифрования

4. Проведена атака на основе знания части открытого текста DEAR ALL THANK YOU FOR. На основе этой части сначала восстановлено слово BEING, затем — на основе расширенного открытого текста — проведена окончательная дешифровка. Результаты на рисунке 11

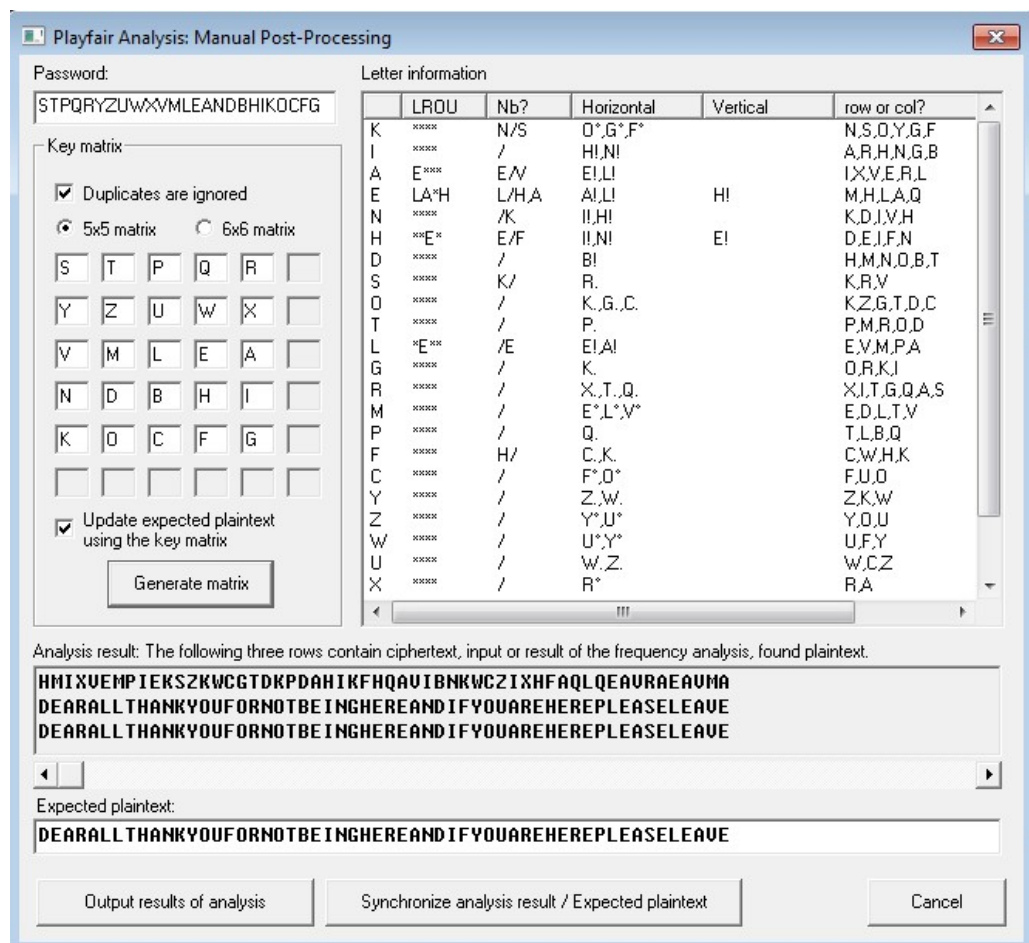


Рисунок 11. Результаты атаки на шифр Плейфера

5. Коллеге зашифрована следующая цитата Ленина ключом STATEANDREVOLUTION: “In capitalist society, under the conditions most favorable to its development, we have more or less complete democracy in the democratic republic. But this

democracy is always restricted by the narrow framework of capitalist exploitation and consequently always remains, in reality, a democracy for the minority, only for the possessing classes, only for the rich. Freedom in capitalist society always remains about the same as it was in the ancient Greek republics: freedom for the slave owners”.

Результат: FT BE HF AE RF TA ED FB NA QC SL TO RW OM LE RU RH LE EG
DE NI VB LV VK ON ER HR DU AO NO LM YO SA YT KT OA YC OT LV ON AQ
EU CY ZF NA SO OY CM VT ME FT RW SO OY CM VT RH IO NM IC RF FC IS
RW UT OS YC IO EB WC TE RZ EX TD NT RI BF AN VU WE MT SE VW VL ZI
VT YO YR VH LC BE HF AE RF TA AY ZF RC AE RH LE ES OU LE TN SG NS
NR XE RZ EX TD OY TB ST FT OT NV HR XE OS YC IO EB ZC LV RW OY FT
LV HR EC LF ZC LV RW NM DE TN AQ TU SP FO ET TN ED LF ZC LV RW TO
BF PI OT SO CY FT BE HF AE RF TA ED FB NA XE RZ EX TD OY TB ST VK
DC AW RW NT EK NE TU RT ET FT RW NE EF CT SA HD AY AM OT GF FV BF
NU OT SO CY CL IR MT ND VB OC ZT TO AQ.

Коллеге переданы следующие слова сначала: INCAPITALISTSOCIETYUNDERTHE

6. Дешифрование полученного текста:

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Выводы

Название шифра	Тип шифра	Ключ
<i>Hill</i>	Замена	Шифрующая матрица
<i>ADFGVX</i>	Комбинированный	Матрица, ключевое слово
<i>Playfair</i>	Замена	Матрица

Название шифра	Сложность brute force
<i>Hill</i>	26^{n^2} , где n — размер матрицы. Если неизвестен, то $n \leq \log_2(l)$, где l — длина сообщения
<i>ADFGVX</i>	$36! \times 36$
<i>Playfair</i>	$25!$