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 _____ Корытов П.В.

Преподаватель _____ 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`

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

Шифротекст: `CPSSQVBUPQFMOFHKKJ`

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

Расшифровка:

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

1.2. 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 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 CrypTool1. 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

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

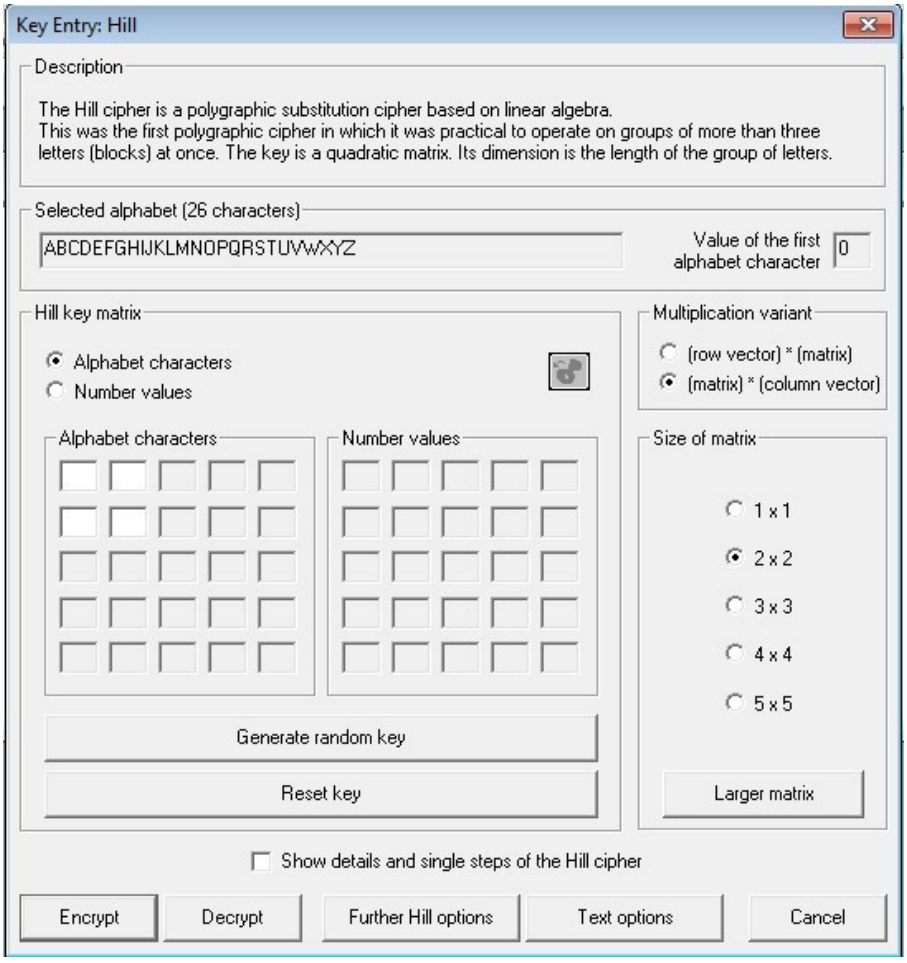

Рисунок 1. Параметры шифра Хилла

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 `JBH WXI JWW`.

   Результат: `HCLQ GL ZCSVLGA BZOSZ KEPXXOBLYOT SMYLO AQJ TCTI JLWO`
4. Проведена атака на основе открытого текста текста. Результаты на рисунке 2
5. Из сообщения удалено ФИО автора. Дешифрованный ключ совпадает с

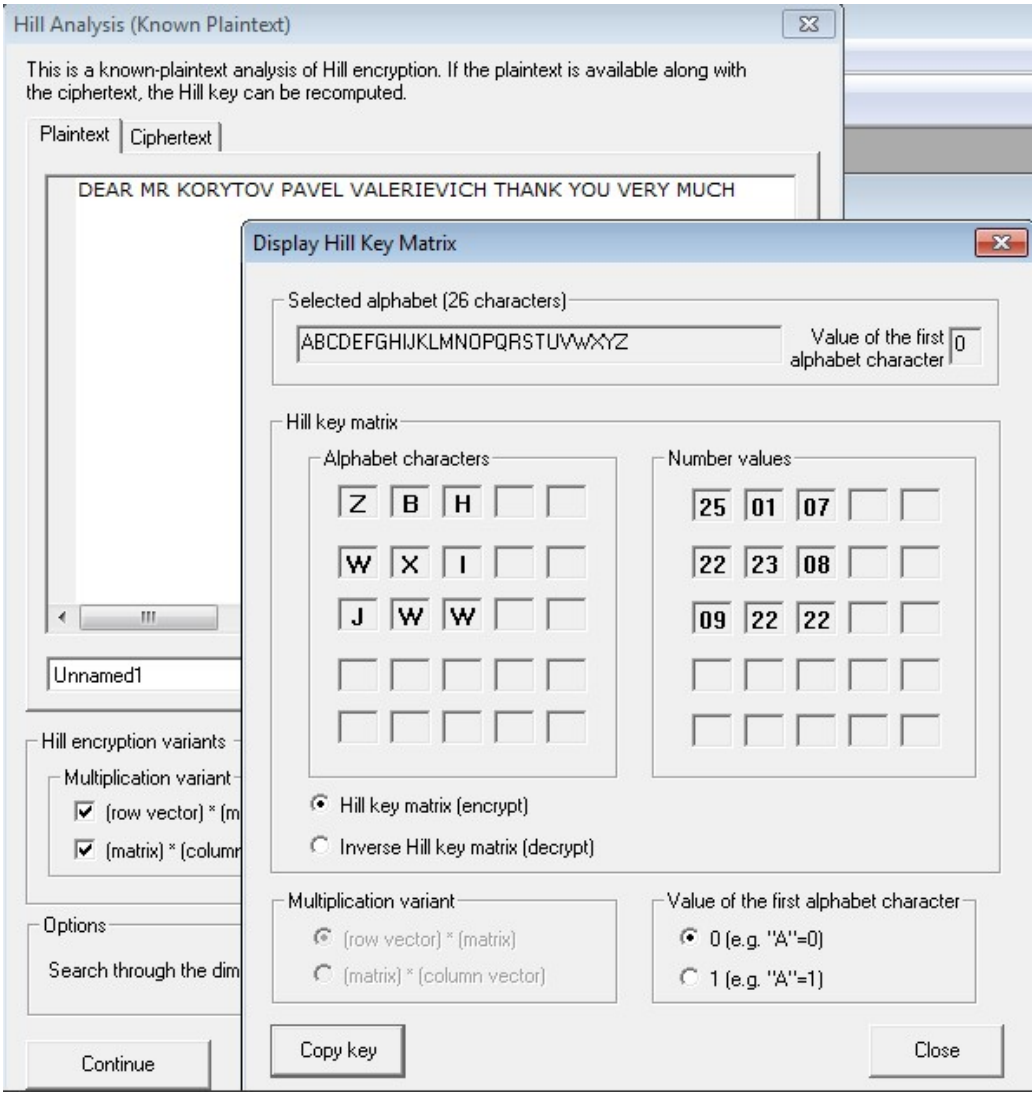

Рисунок 2. Атака на шифр основе открытого текста

исходным

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. Получен следующий шифротекст: `GYHBPUMH XJZHEITSIWUJEFMLVGCQJLBENCMIIX IEFEWOTVFRY XWDETLYOOA`.

   По паре открытый текст / шифротекст — `LADIES AND GENTELM` / `GYHBPUMH XJZHEITSI` — восстановлен ключ — матрица 3×3 `I J F L C J M Y D`.

   Дешифрованный открытый текст: `LADIES AND GENTLEMEN WELCOME TO THE FIRST SATANIST TEMPLE ININIATION CEREMONY THANK YOU`.

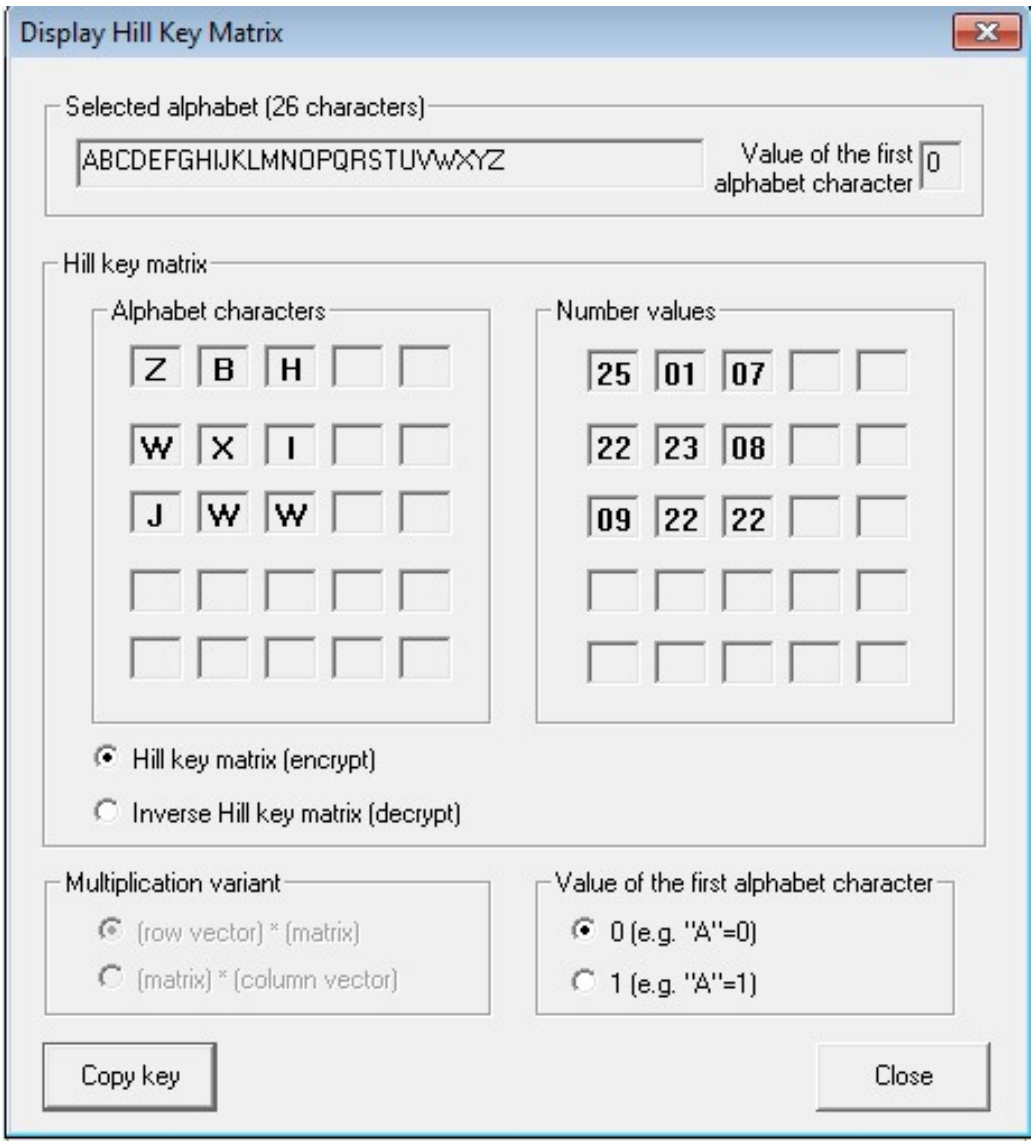

Рисунок 3. Повторение атаки на основе открытого текста

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.

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

Рисунок 4. Первый шаг зашифровки

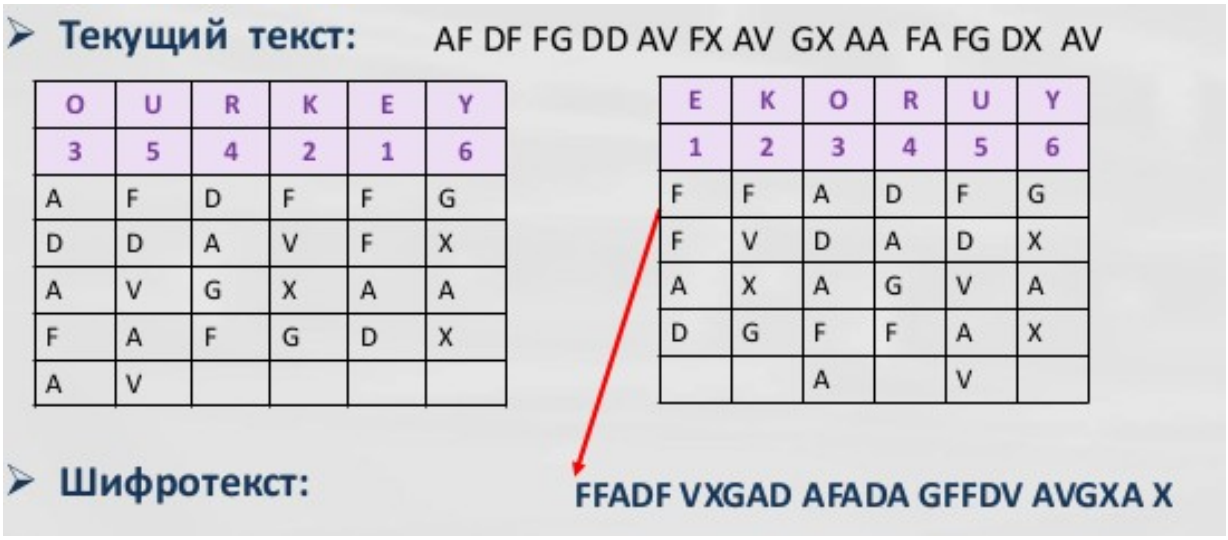

Рисунок 5. Второй шаг зашифровки

/ 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**
4	*1*	*5*	*2*	*3*
D	F	V	V	V
X	F	A	G	D
V	V	G	G	

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

P	**A**	**V**	**E**	**L**
4	**1**	**5**	**2**	**3**
1	*2*	*3*	*4*	*5*
1	**2**	**3**	**4**	**5**
2	*4*	*5*	*1*	*3*
E	*P*	*V*	*A*	*L*

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

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

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

Второй шаг дает исходный текст: KORYTOV

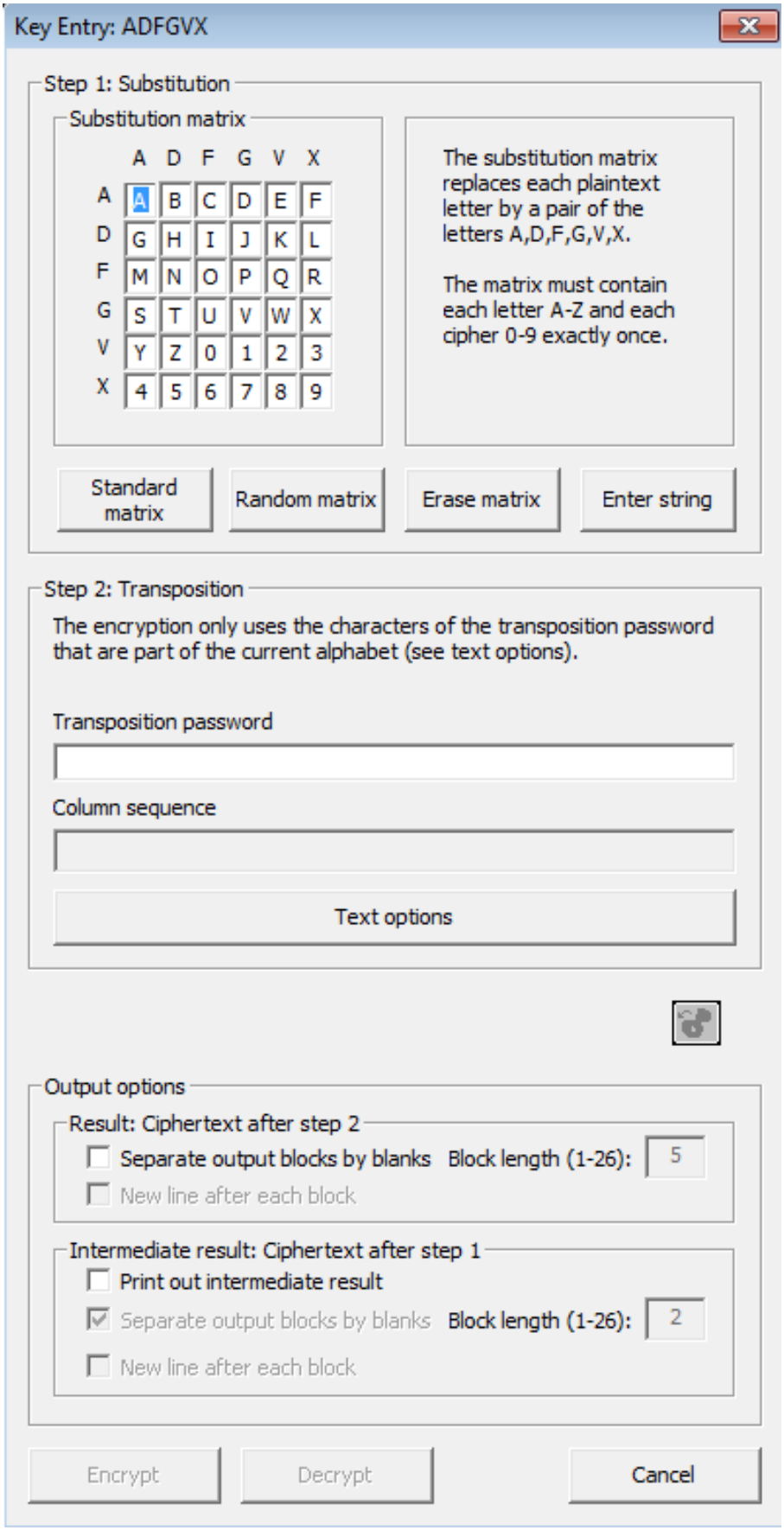

Рисунок 6. Параметры шифра ADFGVX

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

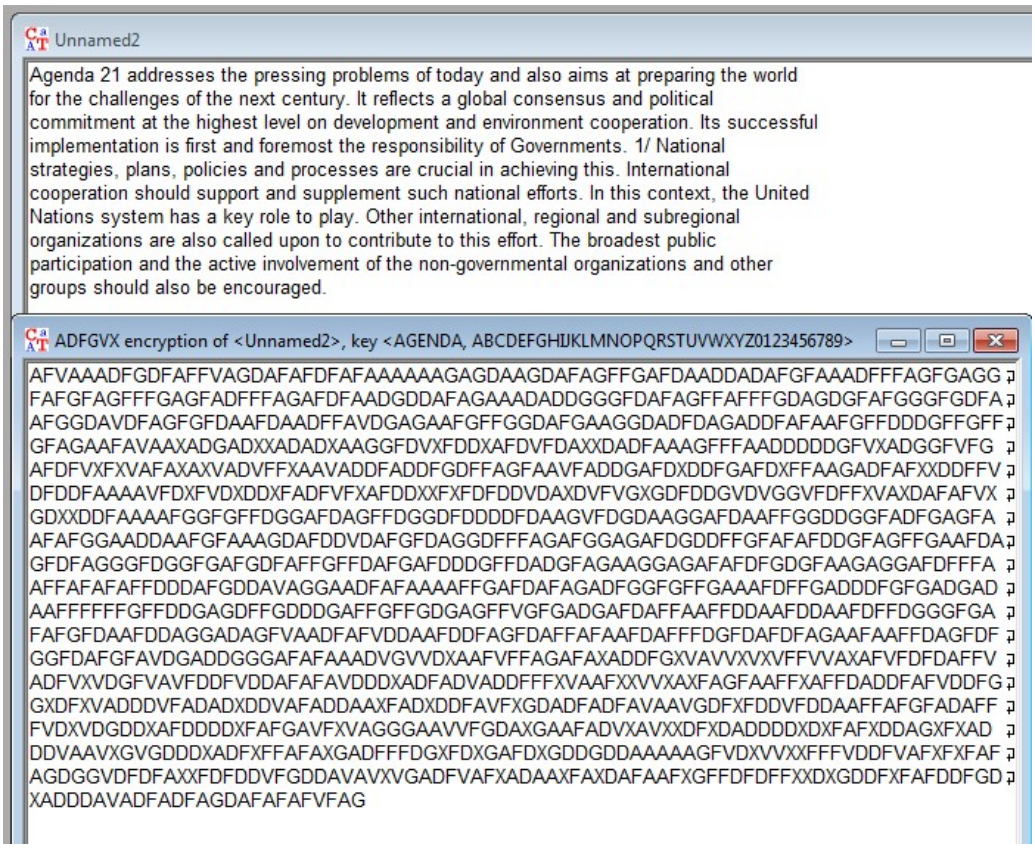

Рисунок 7. Зашифровка абзаца Agenda 21

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.

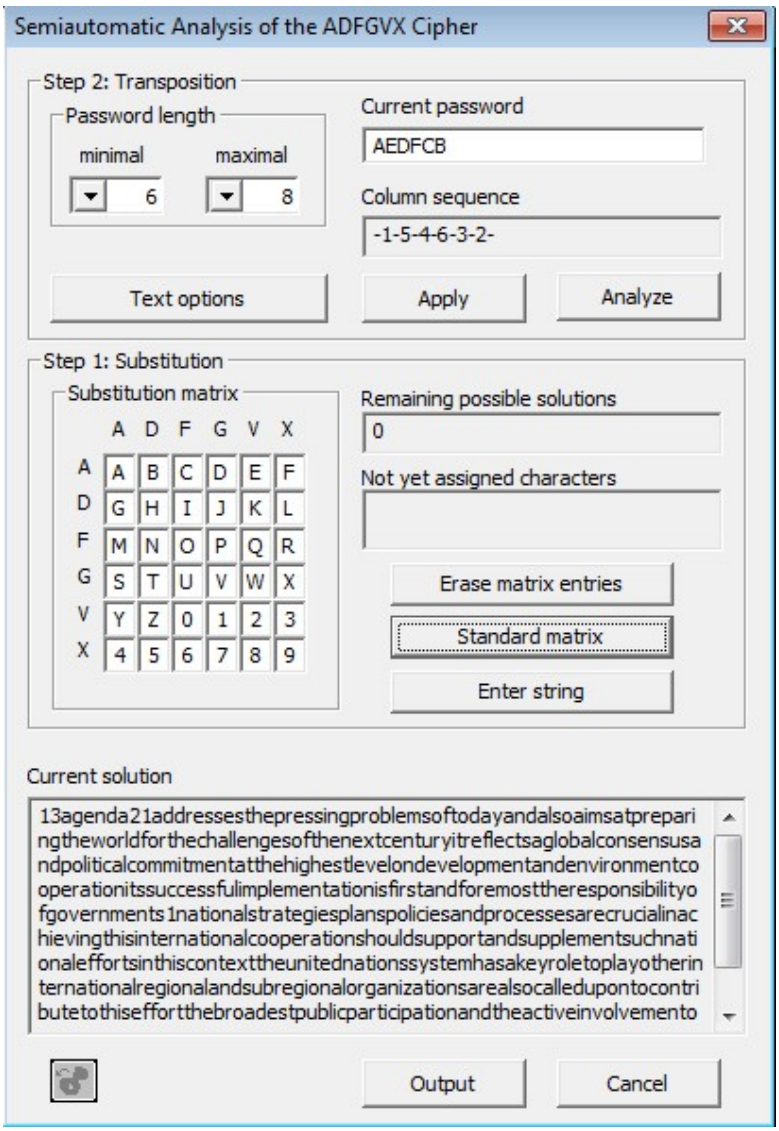

Рисунок 8. Атака на шифр ADFGVX

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 DGAFA ADVVG AFVFV FXGVG VDDFA GAAFA VDDGA DXAXG VADAF AVDAD FDVFA AXDXG DFDAA DDGVA GFFAD GVFVA FADAV DDDVD VDDAA AAFAF AGAAF AGADF AGAAD FADDG GFDFV AFGVA DADAA GAGVG DGVAA FDAFA 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

   От коллеги получен шифротекст: “FFGXX DFXDD DVDXA FFGFF DGDFV XFADD AAADX DDDAD DDFDD FVDXA VAXGX FXADF AFXGF VAGFF AVGGX DFFAF AXVFD FAFAG FDAAG AGFFD FADFD FFDGD AADFA GAGFD FFFFF DFAGD ADFAA FDFFD DGDAG FDAAA GADFG AAGFD AGGFF DADGF ADDGG AAAGF FAAFF AFGFD DGDDF GFFFA GAGAF AAFGA FDDDG AAFGA DAGAA GDDDG AAFAA AFGFA FAGAF FAADD FAVDV FFVFG VVDXF VADDV AAFFA DFXXA FAXXA VDAFV AFDVX FXVDV VXAAX ADFVV FDDFG VXAVV AAGVF VDVFX VXFXD A”

   С помощью атаки по словарю CrypTool2 сообщение восстановлено.

   IWONDERIFITWOULDBEBETTERTOREMAINONDEIMOSHOPINGITWILLCRASHONMARSFASTER

   Расставлены пробелы:

   I WONDER IF IT WOULD BE BETTER TO REMAIN ON DEIMOS HOPING IT WILL CRASH ON MARS FASTER THAN ONE MAN ON THE ORBIT LIKE THERE ARE SMALL PARTICLES WHICH SHOULD DECREASE DEMOS SPEED OVER THE COURSE OF MILLENIA

   Атака заняла продолжительное время; потребовался подбор длины ключа. Было отвергнуто несколько вариантов, которые расшифровывали текст бессмысслицу.

   Предположительно, текст описывает возможности схода со стабильной орбиты Марса без использования реактивной тяги.

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

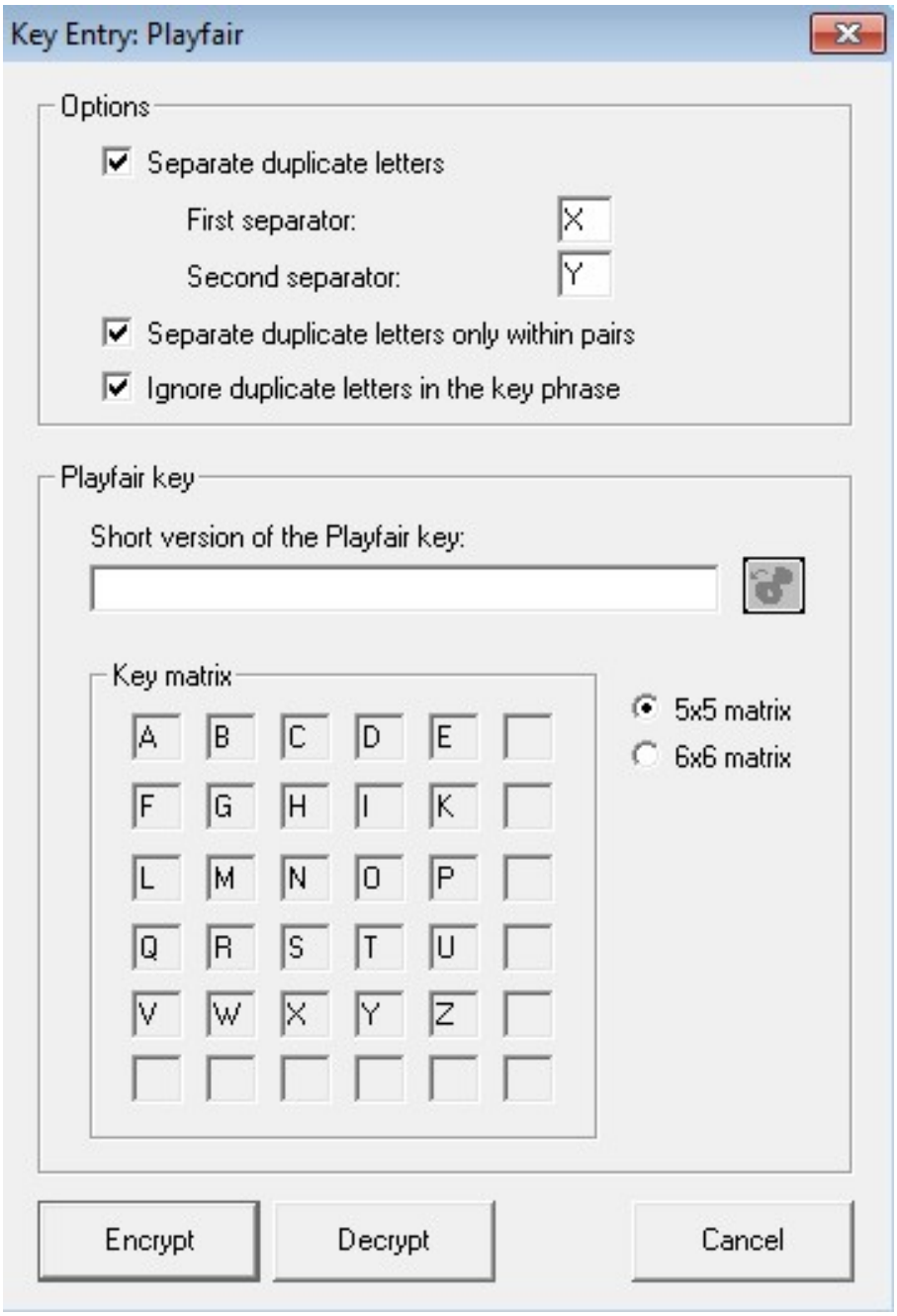

Рисунок 9. Параметры шифра Playfair

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

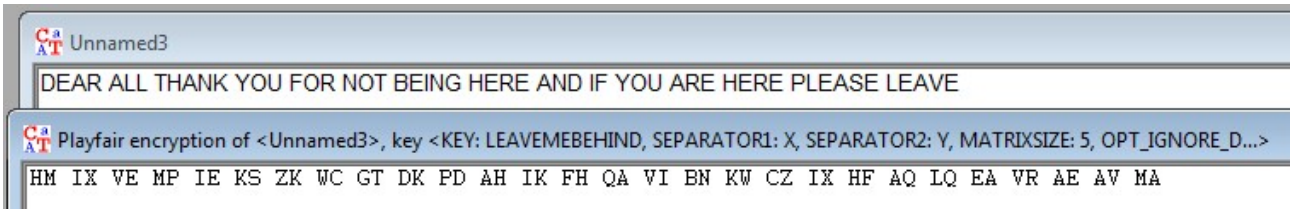

Рисунок 10. Результаты шифрования

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

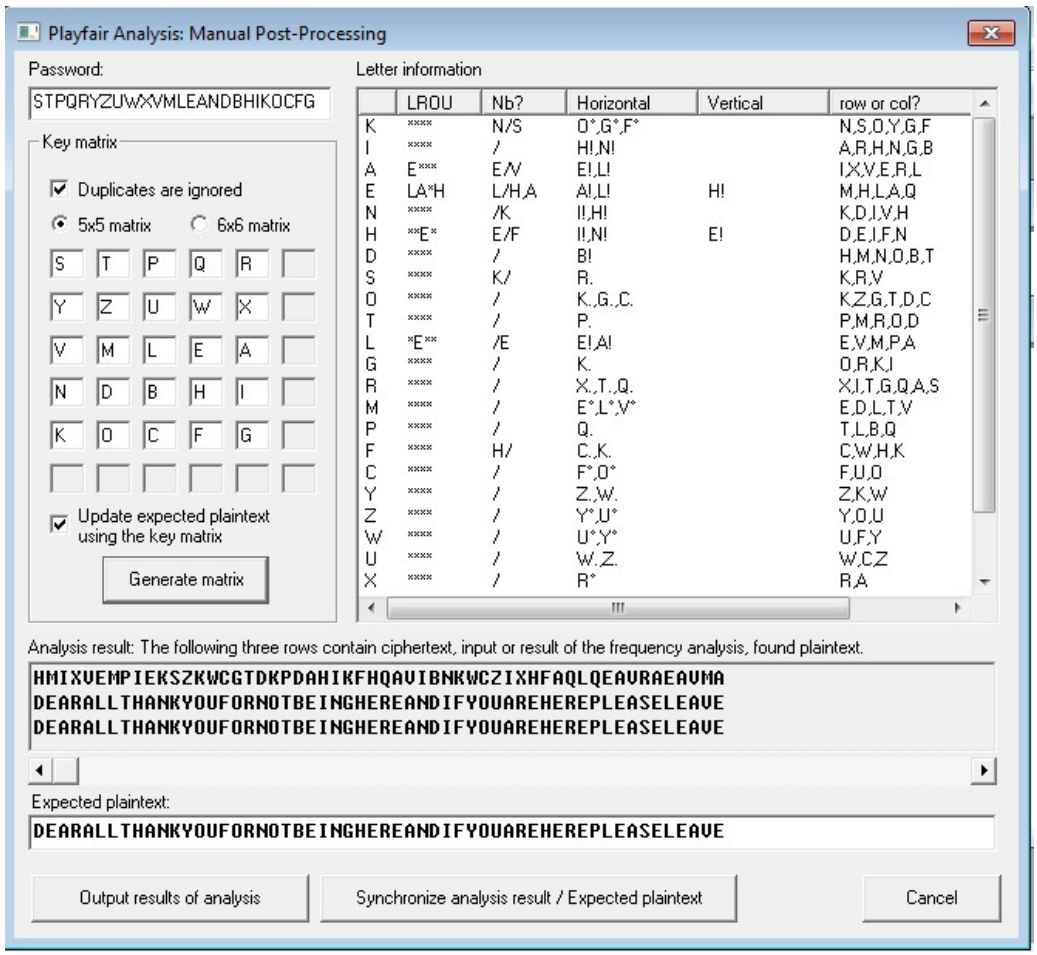

Рисунок 11. Результаты атаки на шифр Плейфера

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. Получен шифротекст: SK CS ON AT PU OA NS UR OK OM AQ SU NO PN PY MO GI BH NR CR SK IA KI CA PC AV EI SK BA MO BA NR CB YI ON IQ HY NA RC SC YE RK HM IP QE OM HC SK CU AD UW VD SC SF RS NR ZQ SH OM AN AT HI IU HI KL NU SE MK CS SH DI BS BU QO CA ZC UO MR SV SK CE HY QN AP SC WQ IA UC CK IH AB CZ ID NO BV ED RH TQ HE AL NE LC MK EY RS EY QC IP YO HN TL SH ZH US QZ SK CU OD MO AN LC MR SK CE HY LC AT SC RH SK HA UF MK IA NR LV HY YH WQ IA UC CK IH SE TL NS ER PL FA BF KS SH VE RC LC RS SV EN MV ID IH TQ HE AL EY SE TL RE TL SH SR LC OZ MO FG MO TQ HE ON RK LO CR IU SU PH UF HK PZ CL SY OU IL TL SH VH IY IS UW IH NR UY MH DM HY LE YI DU HK LC MK TL VS CS SH HI HU AT DR HY DE IS FV RS PV EY ME NR FR AC FG MO NA MO HE QM DM HY LE YI EP UH MO ON BM RB MK CR PN CA BA AY RP LD IA YE RK EP CR KQ SH YS MO QK SR LD EP NS BY LN BA IS ZE PR YH ON MK CS DE TQ AI YI CZ IH YE AR CL HY SU NO AB RN RK HM QV VD ET OU IL QA CA DO MA SE RD MK CA UF HK OM MA PN AN AC IW IA SK EL YO TE MA EU AC FV CL KS SH AN RC QP HY AY SC BG AI NH CR KQ SH TL UD PW SE SR MZ CR PN AN AZ DP BY UE SI YH KZ UR AT NR HL BE YH KZ UR AT CL SO DL LD RD HI RK LE CZ SH WF RC EN RK AN IC FR RC NR YO AL EY SK IA MA NR

TE UF VL EC AM AI DP BY UE SI SK NR SK US SE SR MZ NR HL LC QV PL UF HK IA SK NR SK BH OE PT NR LD EC ID NR QY

Известное обращение: THETRANSFORMATIONFROMSPEAR. После восстановления некоторых слов восстановлен исходный текст (пробелы расставлены):

THE TRANSFORMATION FROM SPEAR TO SWORD BEGAN IN THE 3RD CENTURY BC THE MORE MANEUVERABLE SAMNITES AND GAULS BROKE THEIR HOPLITE PHALANX THE ROMANS DECIDED TO CHANGE THEIR EQUIPMENT NOW ONLY THE BEST MOST EXPERIENCED MEN TRIARII HAD SPEARS ACTING AS A LAST BULWAK AS THEY KEPT THEIR FORMATION THE BEST INSTEAD THE YOUNGER AND LESS EXPERIENCED HASTATI ALTHOUGH THEY INITIALLY CARRIED SPEARS AS HASTA IS THE LATIN WORD FOR SPEAR AND PRINCIPES FOUGHT WITH SWORDS THEY DEVELOPED A NEW AGGRESSIVE FIGHTING STYLE THE DEFENSIVE SHIELD WALL WAS ABANDONED FOR A MORE AGGRESSIVE USE FOR RAMMING INTO ENEMY SOLDIERS AND USING THE SHORT GLADIUS AT EXTREMELY CLOSE RANGE THIS PREVENTED SAMNITE SPEARMEN AND GALLIC SWORDSMEN FROM HAVING ENOUGH ROOM TO MANEUVER THIS WAS COMBINED WITH THE MANIPLE SYSTEM BREAKING THE STIFF PHALANX INTO MANY FLEXIBLE SECTIONS AND SUBSECTIONS IT PAID DIVIDENDS IN THE PUNIC AND MACEDONIAN WARS AS THE ROMANS COULD BE MORE FLEXIBLE THAN THE PHALANX AND STILL TOUGHER THAN THE GAULS AND IBERIANS

Текст описывает, как гастаты вытеснили триариев с передних рядов боевых легионов Римской Республики.

Выводы

Название шифра	**Тип шифра**	**Ключ**
Hill	Замена	Шифрующая матрица
ADFGVX	Комбинированный	Матрица, ключевое слово
Playfair	Замена	Матрица

Название шифра	**Сложность brute force**
Hill	26^{n^2}, где n — размер матрицы. Если неизвестен, то $n \leq \log_2(l)$, где l — длина сообщения
ADFGVX	$36! \times n!$, где n — длина ключа. Если неизвестно — длина сообщения.
Playfair	$m!$, где m — размер матрицы.

Шифр Hill — сложный в использовании из-за обращения матриц. Эту операцию непросто провести вручную (особенно для больших матриц), на вычислительном оборудовании это тоже неэффективно. В то же время, для взлома шифра достаточно решить систему линейных уравнений, зная небольшое количество исходного текста, что является тривиальной задачей.

Шифр ADFGVX — самый криптоустойчивый из рассмотренных. Его ручной взлом затрудняет его комбинированная структура; однако это возможно. На современном вычислительном оборудовании взлом осуществить легко. Увеличение количества шифротекста облегчает взлом, что свидетельствует о плохой масштабируемости решения.

Шифр Playfair — самый простой из рассмотренных. Для его взлома достаточно 15–25 символов с начала текста.