**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра ИБ**

**отчет**

**по лабораторной работе №2**

**по дисциплине «Криптографические методы защиты информации»**

**Тема: Изучение классических шифров Hill, ADFGVX, Playfair**

|  |  |  |
| --- | --- | --- |
| Студентка гр. 4383 |  | Гордеева Т.В. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2017

**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 (Hill)**

**1.1 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 c выбранным ключом 2х2. Убедиться в совпадении результатов. Проверить обратимость шифрующей матрицы (ключа).

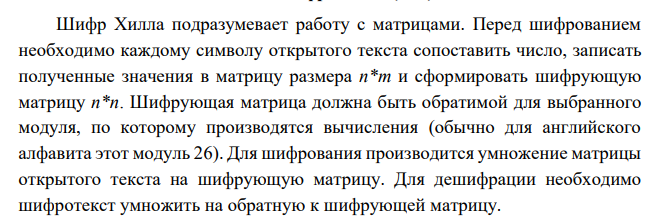
3. Зашифровать текст с произвольным сообщением в формате «DEAR MR ФАМИЛИЯ ИМЯ ОТЧЕСТВО THANK YOU VERY MUCH», используя транслитерацию латиницей и шифрующую матрицу 3х3.

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.

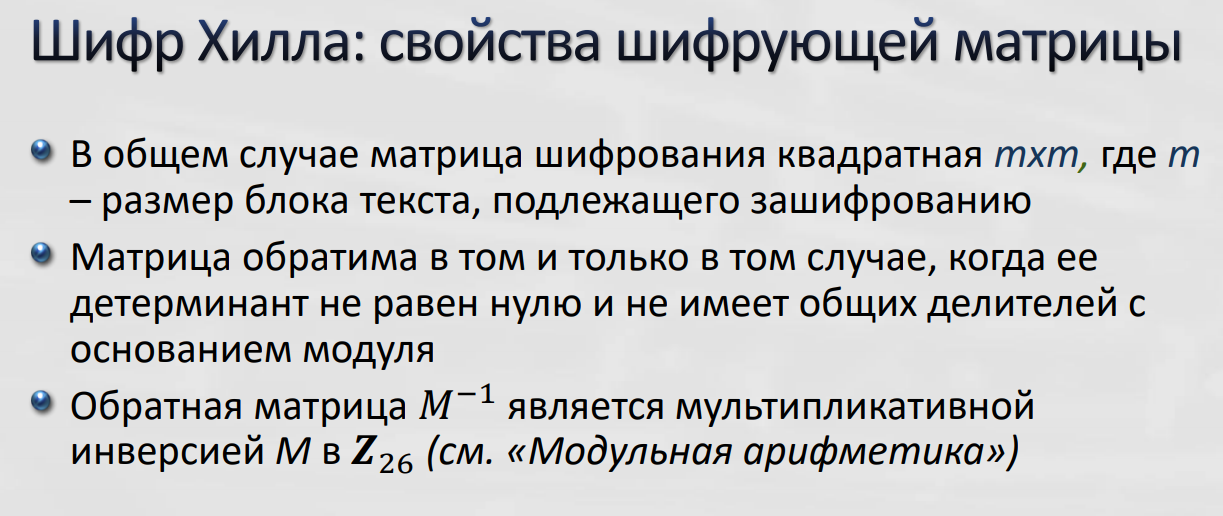
6. Передайте произвольную шифровку коллеге для расшифрования при условии, что формы обращения и завершения сообщения известны. Размер использованного ключа держать в секрете.

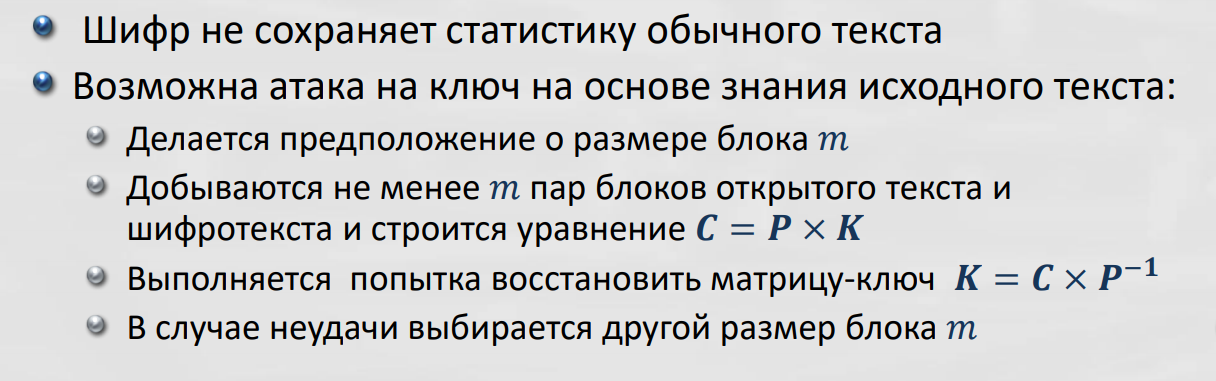
**1.2 Исходное описание шифра (как в лекции). Пример вычисления шифрующей и расшифровывающей матрицы.**

****

****

****

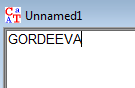
****

****

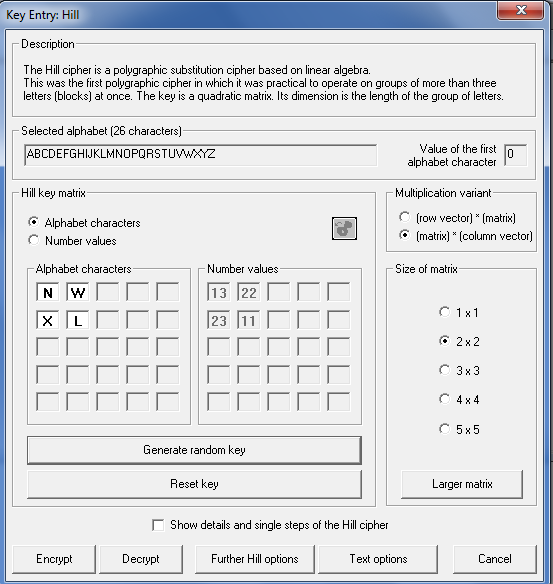
**1.3 Реализация в CrypTool 1.0**

Зашифруем и расшифруем текст содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра c выбранным ключом 2х2.

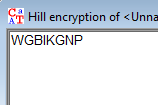
Открытый текст:



Спецификация параметров:



Шифротекст:



Зашифруем и расшифруем текст вручную:

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

Матрица для открытого текста:

|  |  |
| --- | --- |
| 6 | 14 |
| 17 | 3 |
| 4 | 4 |
| 21 | 0 |

Ключ:

|  |  |
| --- | --- |
| 13 | 22 |
| 23 | 11 |

(определитель матрицы -363<>0, следовательно обратная матрица существует)

Перемножим матрицы:

|  |  |
| --- | --- |
| 386 | 292 |
| 287 | 424 |
| 140 | 136 |
| 273 | 483 |

Возьмем полученную матрицу по модулю 26:

|  |  |
| --- | --- |
| 22 | 6 |
| 1 | 8 |
| 10 | 6 |
| 13 | 15 |

Шифротекст:

WGBIKGNP

Дешифрующая матрица:

|  |  |
| --- | --- |
| 11 | 3 |
| 4 | 13 |

Перемножим матрицы:

|  |  |
| --- | --- |
| 266 | 144 |
| 43 | 107 |
| 134 | 108 |
| 203 | 260 |

Возьмем полученную матрицу по модулю 26:

|  |  |
| --- | --- |
| 6 | 14 |
| 17 | 3 |
| 4 | 4 |
| 21 | 0 |

Полученный открытый текст: GORDEEVA

Полученный открытый текст совпадает с исходным.

**1.4 Тип шифра**

Тип шифра – замена, блочный.

**1.5 Ключ шифра**

Ключ шифра – шифрующая матрица.

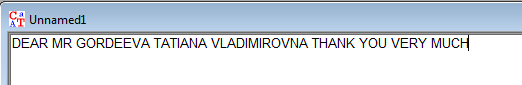
**1.6 Оценка сложности атаки “грубой силы”**

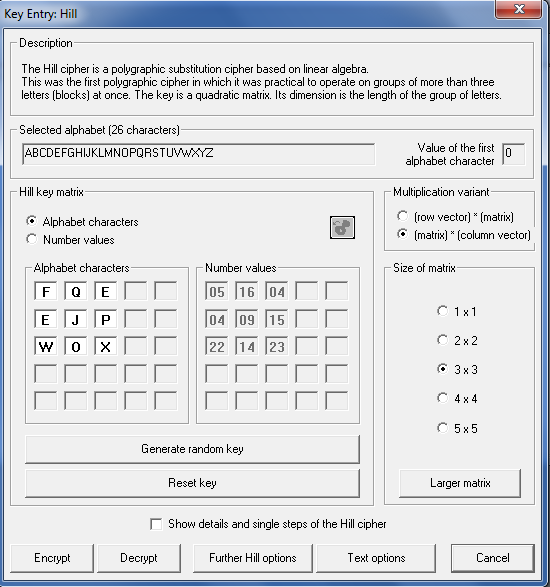
Сложность атаки методом «грубой силы» в худшем случае nm\*m

**1.7 Описание атаки на шифр с использованием утилит Cryp Tool 1.0.**

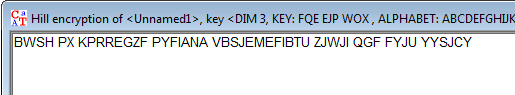
Зашифруем текст с произвольным сообщением в формате «DEAR MR ФАМИЛИЯ ИМЯ ОТЧЕСТВО THANK YOU VERY MUCH», используя транслитерацию латиницей и шифрующую матрицу 3х3.

Открытый текст:

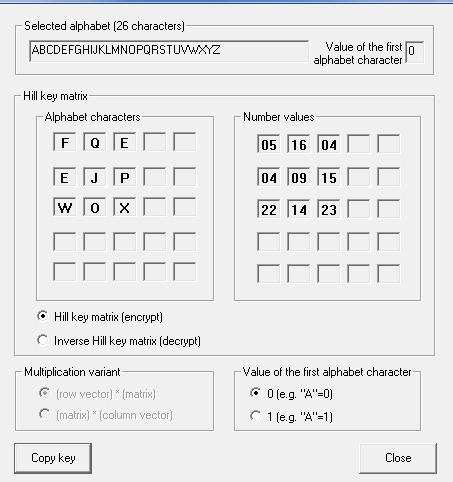




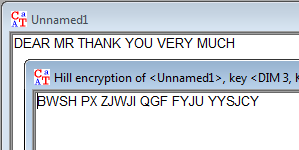
Шифротекст:



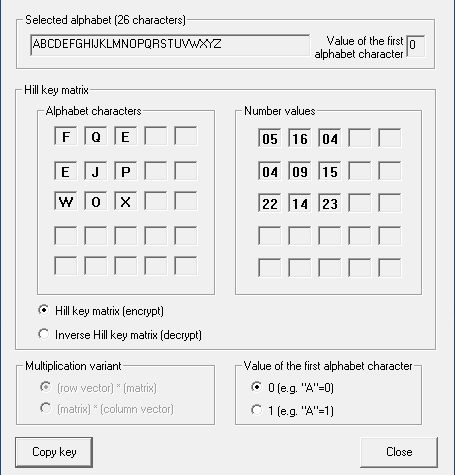
Выполним атаку на основе знания открытого текста, используя приложение из Analysis-> Symmetric Encryption(classic)-> Known Plaintext.



Удалим из сообщения и шифротекста фрагменты с ФАМИЛИЯ ИМЯ ОТЧЕСТВО и повторим атаку.



Полученный ключ:



Полученный ключ (матрица) совпадает с исходным.

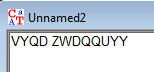
**1.8 Результат атаки и расшифровка перехваченного от коллеги текста.**

Текст шифровки:

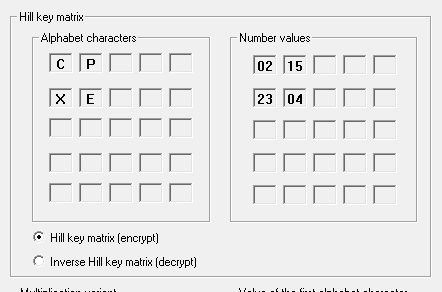


Открытый текст начинается с HELLO и заканчивается на THANKS.

Удалим неизвестную часть:



Выполним атаку на основе открытого текста:



Дешифруем полученное сообщение.

Полученный текст:



**2 Комбинированный шифр ADFGVX**

**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 c 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.

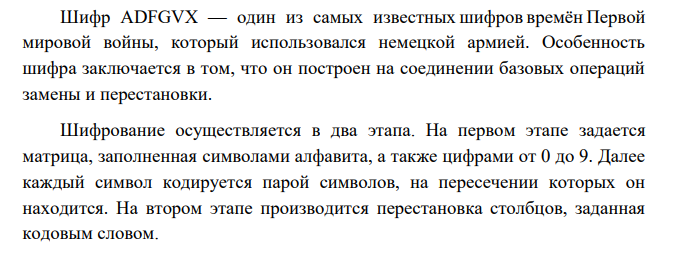
5. Повторить шифрование и атаку для тестов примерно в 300 и в 150 символов.

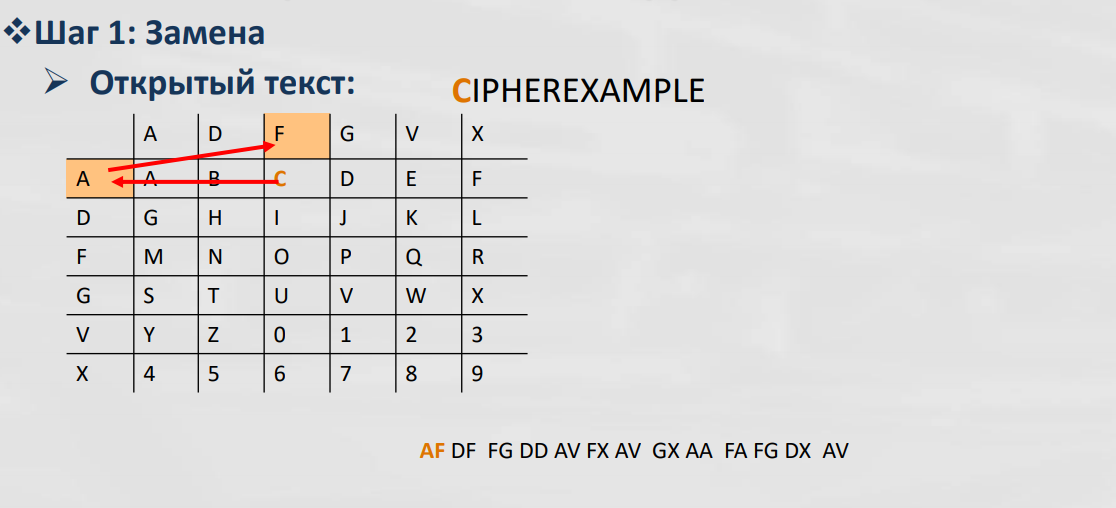
6. Изучите ручное расшифрование для текстов менее 300 символов.

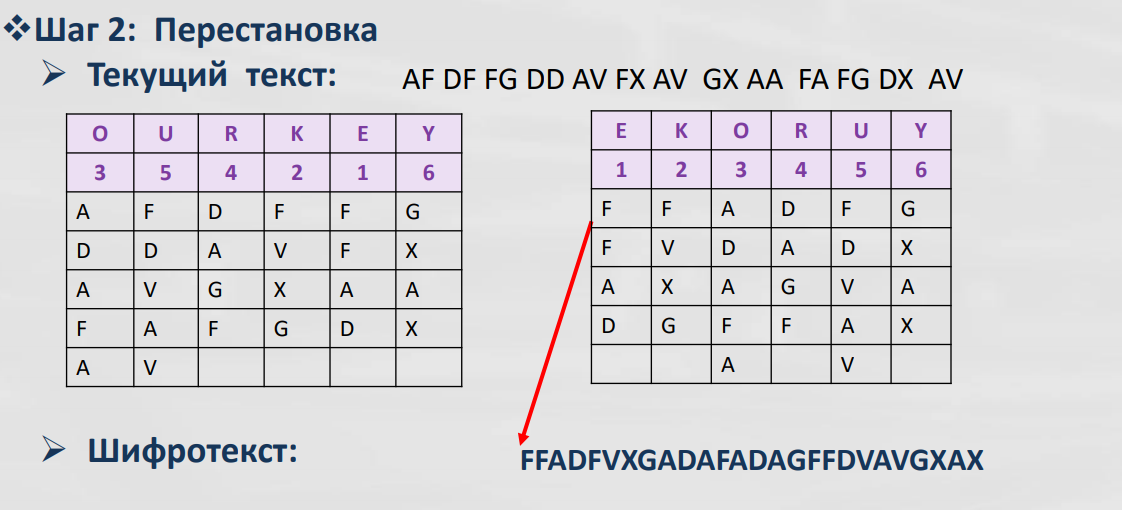
7. Зашифруйте текст из 200 символов, сохраните ключ, и передайте соседу для расшифровки.

8. Самостоятельно изучите атаку по словарю, реализованную в CrypTool 2, опираясь на Help и ссылки на статьи.

**2.2 Исходное описание шифра (как в лекции).**





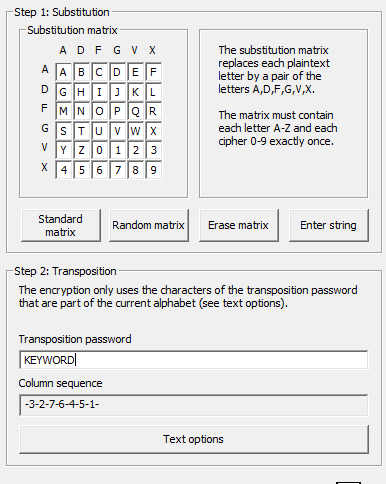


**2.3 Реализация в CrypTool 1.0**

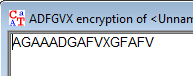
Открытый текст:



Спецификация параметров:



Полученный шифротекст:



Зашифруем данный открытый текст вручную:

Шаг 1

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

Полученная последовательность: DA FF FX AG AV AV GG AA

Шаг 2

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| K | E | Y | W | O | R | D |
| 3 | 2 | 7 | 6 | 4 | 5 | 1 |
| D | A | F | F | F | X | A |
| G | A | V | A | V | G | G |
| A | A |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| D | E | K | O | R | W | Y |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| A | A | D | F | X | F | F |
| G | A | G | V | G | A | V |
|  | A | A |  |  |  |  |

Полученный шифротекст: AGAAADGAFVXGFAFV

Расшифровка будет происходить в обратном порядке.

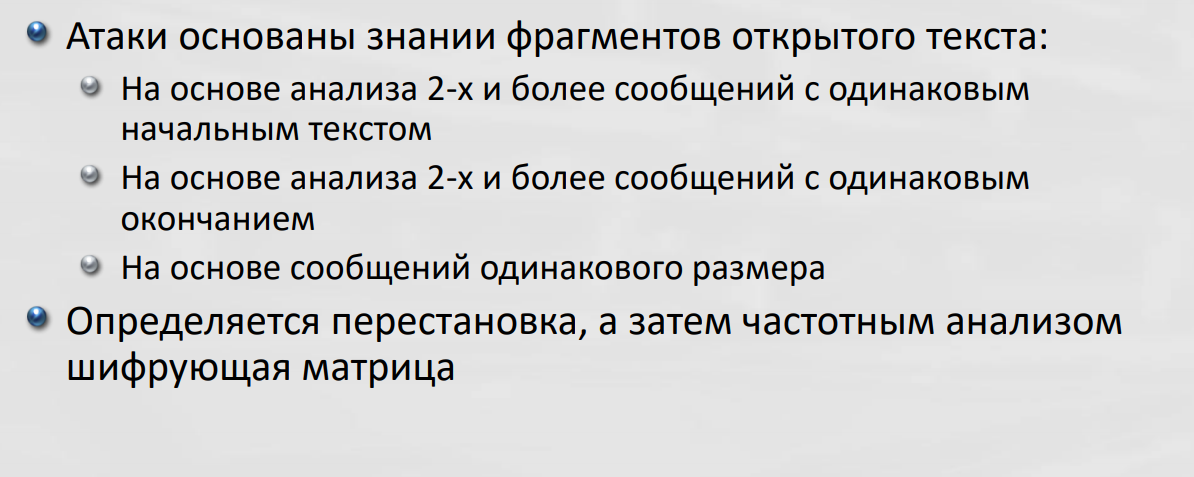
**2.4 Тип шифра**

Тип шифра – комбинированный.

**2.5 Ключ шифра**

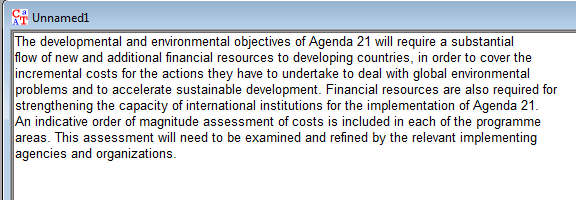
Ключ шифра – матрица замены и ключевое слово.

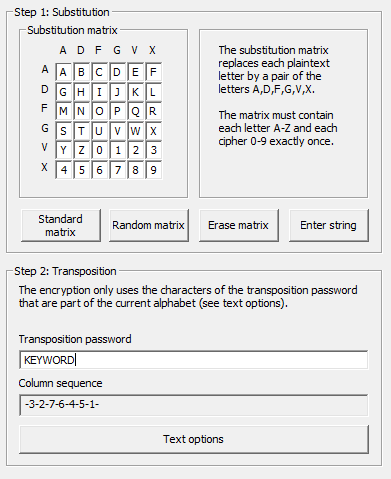
**2.6 Оценка сложности атаки “грубой силы”**

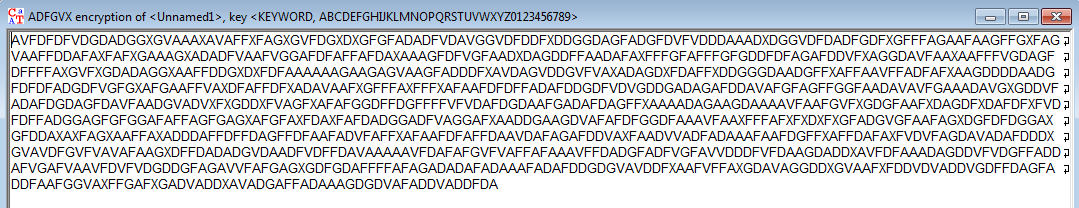


**2.7 Описание атаки на шифр с использованием утилит Cryp Tool 1.0.**

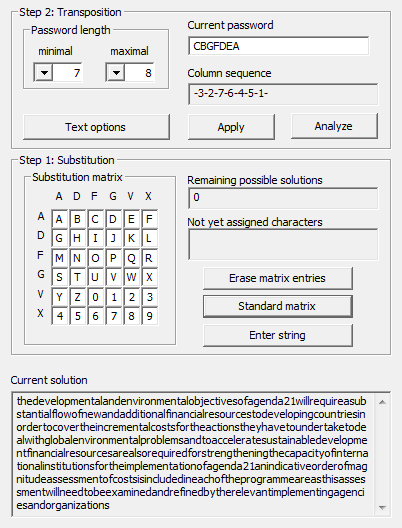
Выберем абзац (примерно 600 символов) из файла English.txt (папка CrypTool/reference) и зашифруем его.



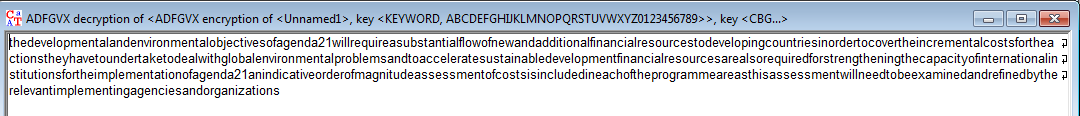




Выполним атаку на шифротекст, используя приложение из Analysis-> Symmetric Encryption(classic)-> Cipher Text Only.

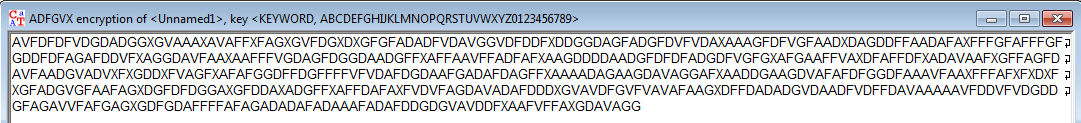


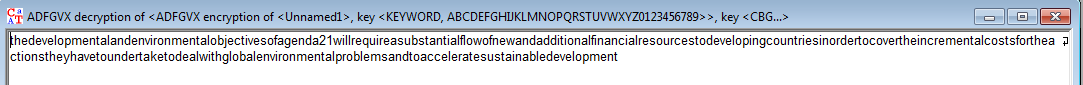
Получен следующий открытый текст:



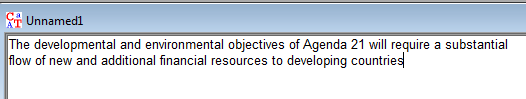
Повторим шифрование и атаку для тестов примерно в 300 и в 150 символов.

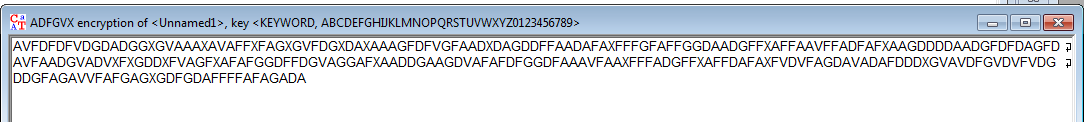
Текст в 300 символов:

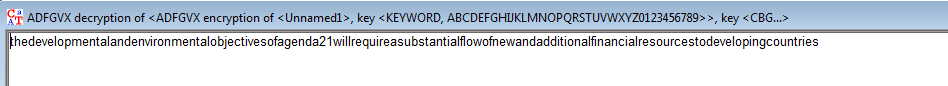


****

Текст в 150 символов:



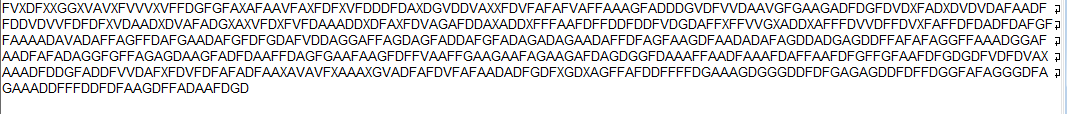


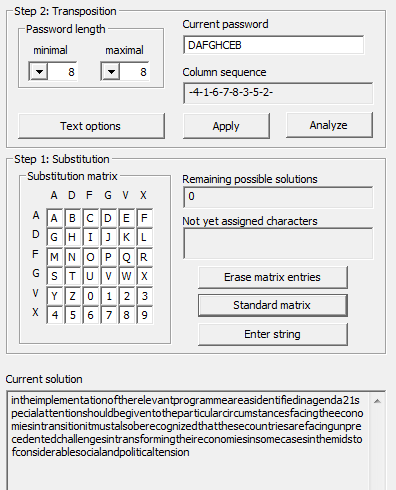


Небольшие тексты требуют большего перебора перестановок.

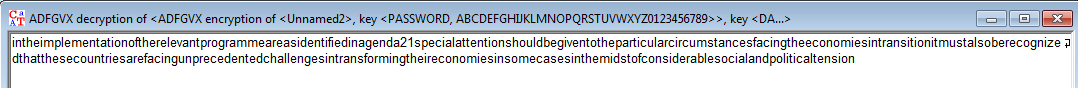
**2.8 Результат расшифровки перехваченного от коллеги текста.**

Полученный шифротекст:

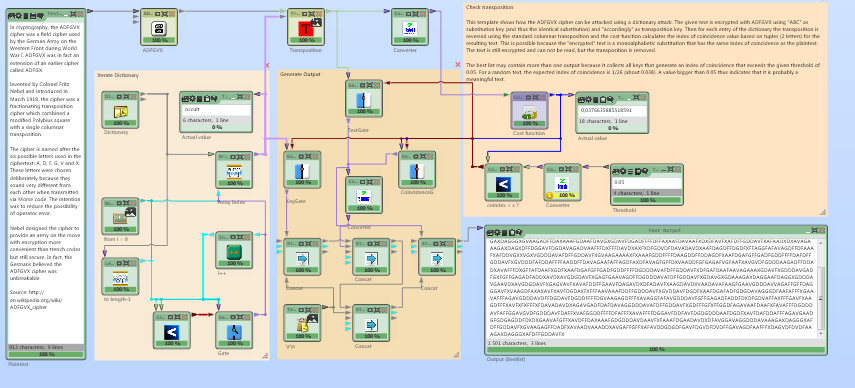




Дешифрованный текст:



**2.9 Описание атаки на шифр реализованной в CrypTool 2.0.**

****

**3 Шифр Плейфера (Playfair)**

**3.1 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 c 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

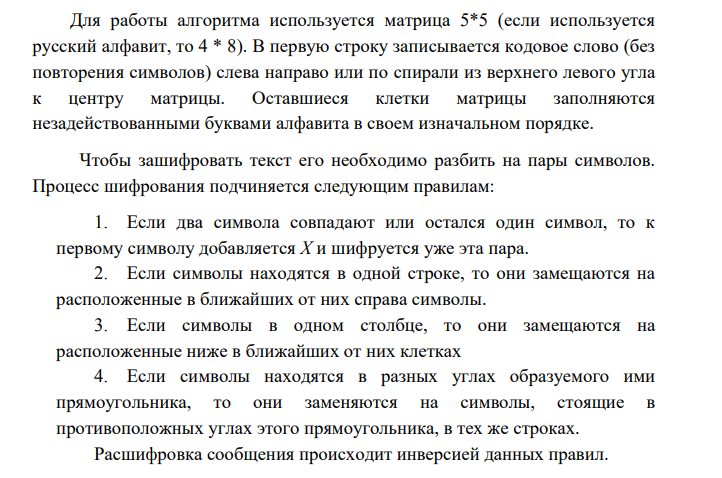
b. Познакомьтесь со спецификацией приложения для проведения атаки в разделе Analysis-> Symmetric Encryption(classic)- >Manual Analysis->Playfair

5. Передайте произвольную шифровку соседу для расшифрования при условии, что форма обращения, используемая в сообщении, известна.

Размер использованной матрицы (ключа) держать в секрете.

**3.2 Исходное описание шифра (как в лекции).**

****

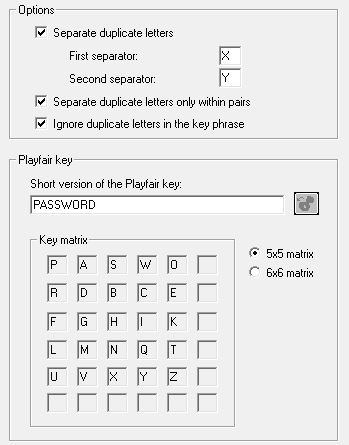
****

**3.3 Реализация в Cryp Tool 1.0**

Открытый текст:



Спецификация параметров:



Полученный шифротекст:



Зашифруем данный открытый текст вручную:

GORDEEVA

GO RD EE VA

GO RD EX EV AX

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

Полученный шифротекст: KA DB BZ DZ SV

Расшифровка сообщения происходит инверсией данных правил.

**3.4 Тип шифра**

Тип шифра – замена/блочный.

**3.5 Ключ шифра**

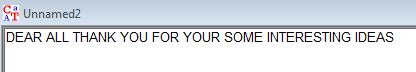
Ключ шифра – ключевая матрица.

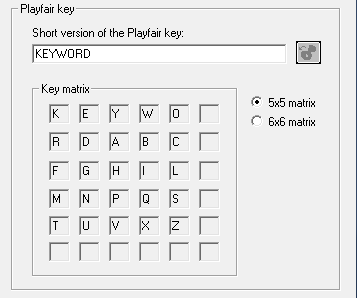
**3.6 Оценка сложности атаки “грубой силы”**

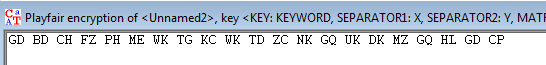
Сложность атаки “грубой силы” 25! для матрицы 5\*5.

**2.7 Описание атаки на шифр с использованием утилит Cryp Tool 1.0.**

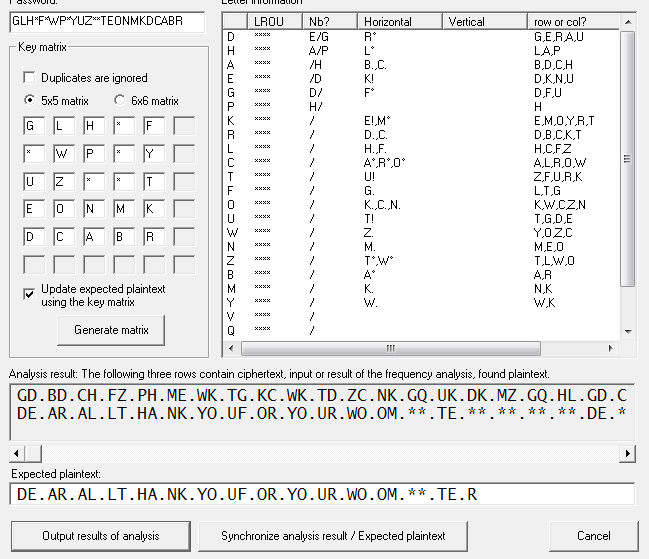
Зашифруем текст с произвольным сообщением в формате «DEAR ALL THANK YOU FOR ПРОИЗВОЛЬНЫЙ ТЕКСТ», используя выбранную шифрующую матрицу.







Выполним атаку на основе знания части открытого текста, используя приложение из Analysis-> Symmetric Encryption(classic)->Manual Analysis. В качестве известного фрагмента текста используем «DEAR ALL THANK YOU FOR»



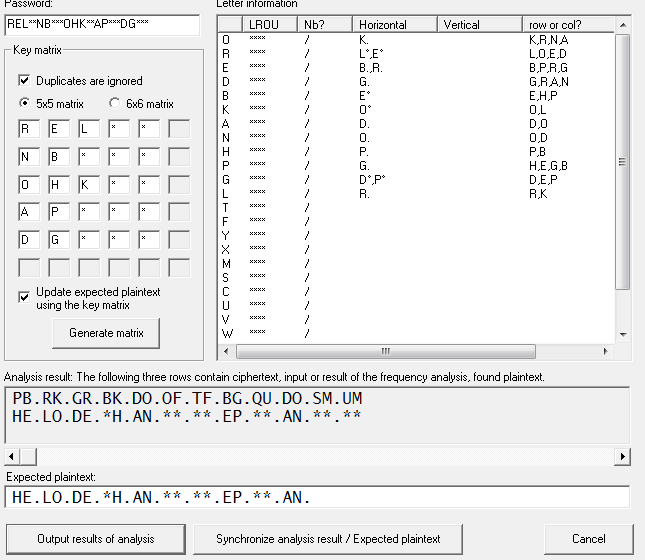
Удалось расшифровать всего несколько символов.

**2.7 Результат атаки и расшифровка перехваченного от коллеги текста.**

Получен следующий шифротекст:



Известно начало текста: HELLO DEAR TANYA



Дешифрованный текст:



**4 Вывод**

В ходе выполнения данной лабораторной работы были изучены с помощью средств CrypTool 1 и CrypTool 2 классические шифры: Hill, ADFGVX, Playfair

Результатом данной лабораторной работы стало изучение алгоритмов шифровки и дешифровки сообщений, также произведена оценка сложности атаки “грубой силой” для каждого шифра.

Для каждого шифра получили следующие выводы:

* Шифр Hill

Тип шифра – замена, блочный.

Ключ шифра – шифрующая матрица.

Сложность атаки методом «грубой силы» в худшем случае nm\*m

* Шифр ADFGVX

Тип шифра – комбинированный.

Ключ шифра – порядок матрица замены и ключевое слово.

Тексты с меньшим количеством символов требуют большего количества переборов перестановок при дешифровке.

* Шифр Playfair

Тип шифра – замена/блочный.

Ключ шифра – ключевая матрица..

Сложность атаки “грубой силы” 25! для матрицы 5\*5.

**Список источников**

* А. К. Племянников, Е.О. Кузнецова Криптографические методы защиты информации: лабораторный практикум. СПбГЭТУ «ЛЭТИ», 2016 55 с.