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

ОТЧЕТ

по лабораторной работе №1
по дисциплине «Криптография и защита информации»
Тема: Шифры Сцитала, Виженера, Playfair
Вариант 0

Студент гр. 8383 _____ Ларин А.

Преподаватель _____ Племянников А.К.

Санкт-Петербург
2021

Цель работы

Изучить принцип шифров Сцитала, Виженера, Playfair, научиться использовать их для зашифровки и расшифровки текстов

Задание

Scytale:

1. Найти шифр в CrypTool 1: Encrypt/Decrypt-> Symmetric(Classic).
2. Создать файл с открытым текстом, содержащим последовательность цифр.
3. Запустить шифр и выполнить зашифровку и расшифровку созданного текста несколько раз.
4. Установить, как влияют на шифрование параметры Number of Edges и Offset.
5. Зашифровать и расшифровать текст содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра при Number of Edges > 2, Offset ≥ 2. Убедиться в совпадении результатов.
6. Взять в CrypTool 2 шаблон атаки на шифр методом «грубой силы» и модифицировать этот шаблон, заменив блок с шифротекстом на блок ввода открытого текста

Vigenere:

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. Произвести атаку на шифротекст, используя приложение Analysis- > Symmetric Encryption(Classic)-> Cipher Text Only->Vigenere.
4. Повторить атаку для фрагмента текста из файла English.txt (папка CrypTool/reference). Размер текста не менее 1000 символов.
5. Воспроизведите эту атаку в автоматизированном режиме:
   a. Определите размер ключа с помощью приложения Analysis- > Tools for Analysis-> Autocorrelation
   b. Выполните перестановку текста с размером столбца равным размеру ключа приложением Permutation/Transposition
   c. Определите очередную букву ключа приложением Analysis- > Symmetric Encryption(Classic)-> Cipher Text Only->Caesar.
6. Самостоятельно изучить атаку, реализованную в CrypTool 2, опираясь на Help и ссылки на статьи.

Playfair:

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. Передать произвольную шифровку коллеги по группе для расшифрования при условии, что форма обращения, используемая в сообщении, известна. Размер использованной матрицы (ключа) держать в секрете.

Выполнение

Вид программы CrypTool 1.4 с первым экспериментов представлен на рис. 1

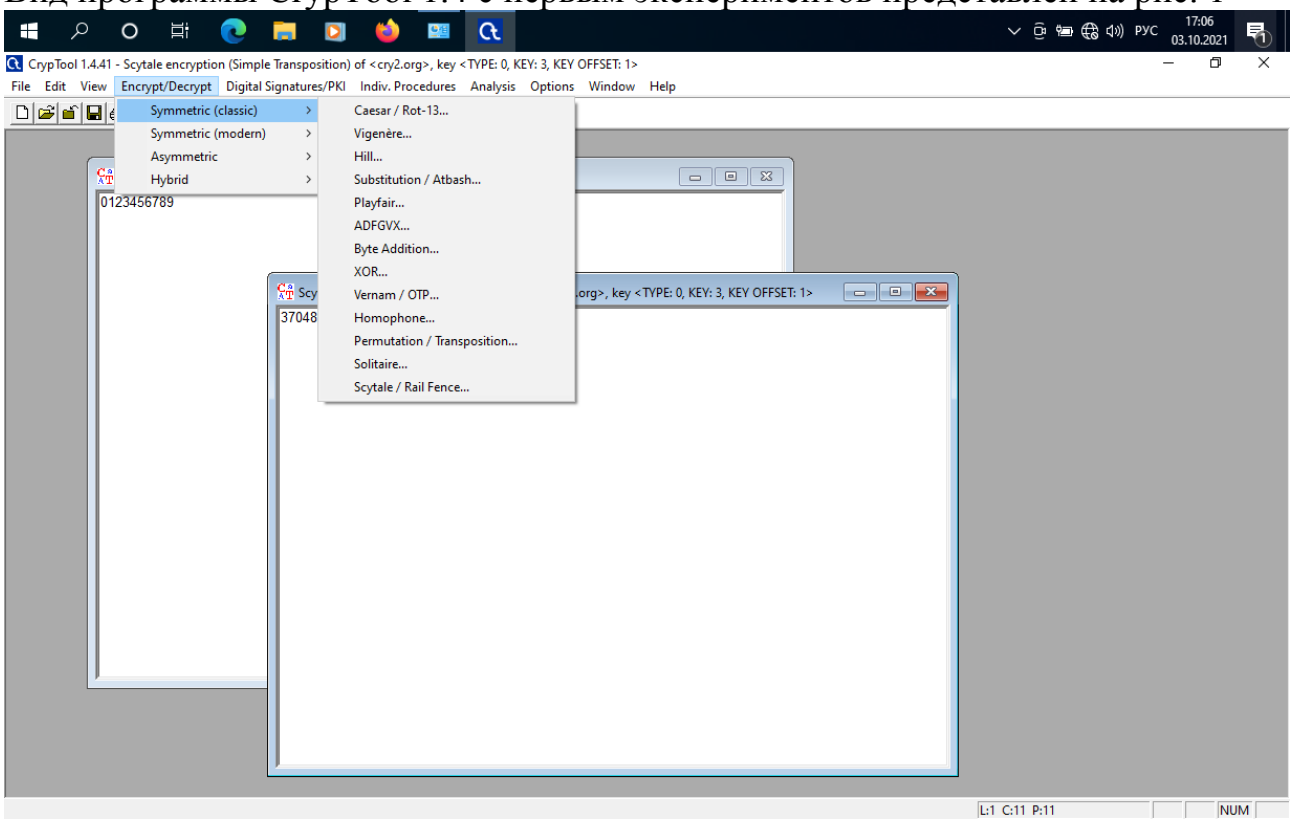


Рисунок 1. Интерфейс CrypTool 1.4

Scytale

Шифр Сцитала относится к шифрам с заменой. Он основан на записи текста на цилиндре с многогранником в основании. На цилиндр наматывается лента пишущей бумаги, на которую записываются символы вдоль каждой из граней по очереди. После размотки ленты на ней получается шифротекст. Для расшифровки требуется цилиндр с тем же количеством граней, следовательно количество граней и отступ являются ключем.

1. Проверка на последовательности цифр
    1. Взята последовательность `0123456789`.
    2. После зашифровки с параметрами `n of edges` = 3, `offset` = 1 получен текст `3704815926`. Последовательные символы разнесены через два, согласно параметру (`n of edges - 1`), первый символ отстоит от начала на одну длину окружности, согласно `offset`. После расшифровки получаем исходный рекст.
    3. После зашифровки с параметрами `n of edges` = 2, `offset` = 0 получен текст `0516273849`. Последовательные символы разнесены через один, согласно параметру `n of edges`, первый символ отстоит от начала на одну длину окружности, согласно `offset`. После расшифровки получаем исходный рекст.
2. Сверка с ручным шифром. `Larin. Offset = 1, n_of_edges = 3`
    1. Начальный символ сдвигается на две позиции
       `__L__`
    2. Остальные распологаются каждую вторую последовательно
       `a_L__`
       `a_Lr_`
       `aiLr_`
       `aiLrn`
    3. Зашифровка при помощи CrypTool дала тот же результат
3. Взлом шифра методом грубой силы
    1. Был взят стандартный иниструмент для взлома Scytale, после чего блок с шифротекстом был заменен на блок ввода текста и блок зашивровки. Вид схемы приведен ниже. В качестве текста был взят параграф с википеди. В результате текст был корректно расшифрован.

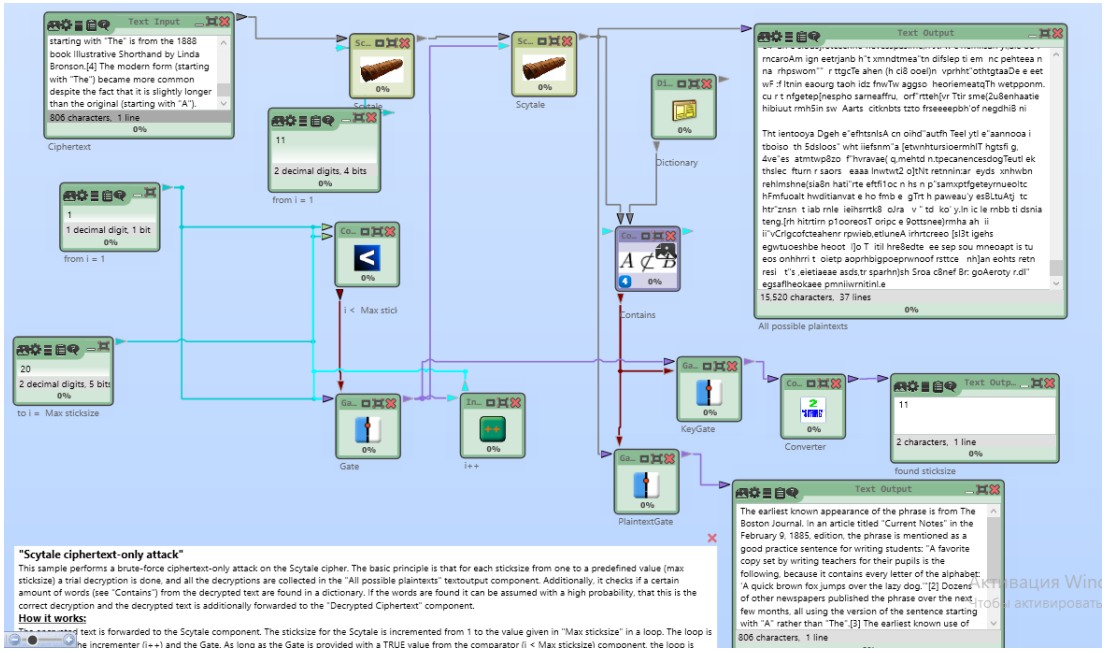


Рисунок 2. Видсхемы для взлома Scytale методом грубой силы

2. Данный вид взлома работает при помоще перебора параметров, формирования списка всех возможных вариантов и выбора самого реалистичного. Самый реалистичный вариант выбирается методом сверки слов результата со словарем

Vigenere

Шифр Виженера - метод полиалфавитного шифрования текста с использованием ключевого слова. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера.

Выбирается кодовое слово длины n, которое делит открытый текст на отрезки данной длины. Далее составляется, так называемая, таблица Виженера. Горизонтально записывается алфавит, вертикально под первым символом алфавита записывается кодовое слово. Заполнение таблицы осуществляется символами алфавита, начинающегося с элемента кодового слова, и циклически замыкается (т.е. применительно к латинице это выглядит так: ...xyzabc...). Элемент шифротекста выбирается на пересечении столбца, соответствующего букве открытого текста и строки, соответствующей букве кодового слова.

1. Был зашифрован текст с фамилией `larin` вручную и при помощи cryptool.
   В качества ключа взяты символы раскладки `qwerty`
2. Результирующий шифротекст совпал, результат представлен на рис. 3

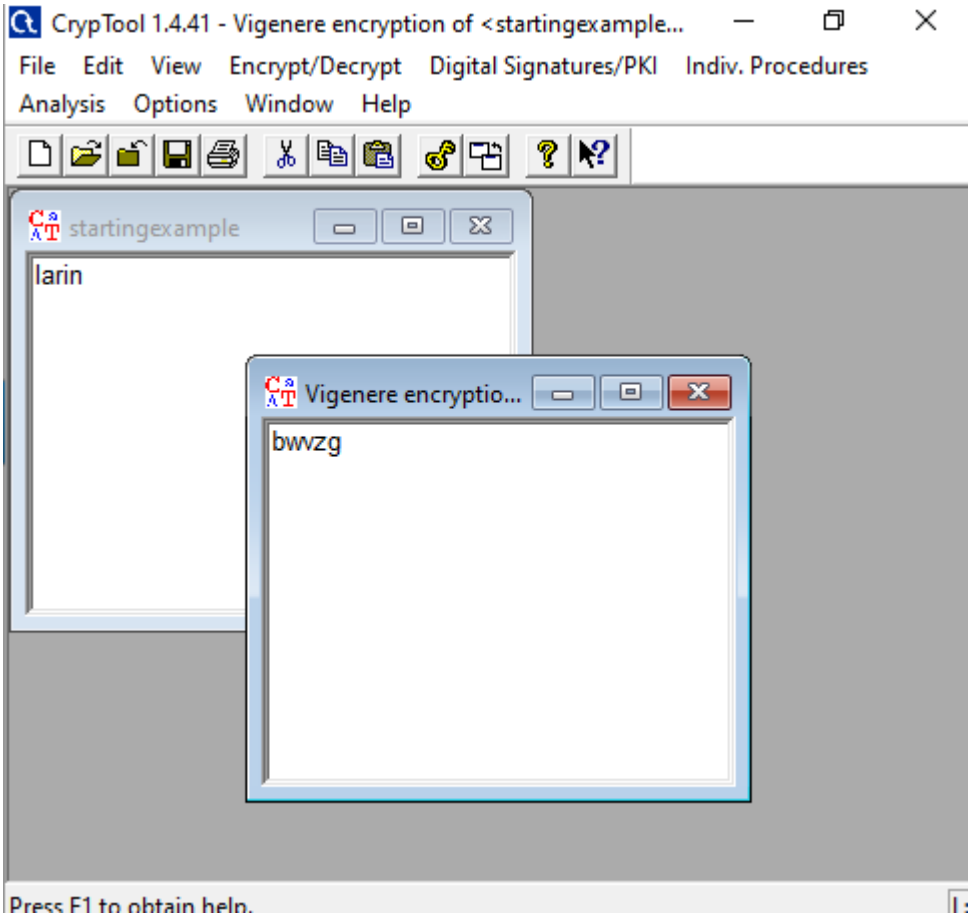


Рисунок 3. Шифр Виженера

3. Для анализа необходимо не менее восьмисимволов, потому взят текст `larin anton` (с пробелом в алфавите и тексте). Шифротекст: `awvzfxqixef`
4. Выполнен анализ инструментом Analysis -> Symmetric Encryption(Classic) -> Cipher Text Only →Vigenere
   Длина ключа 5
   Результат на рис. 4.

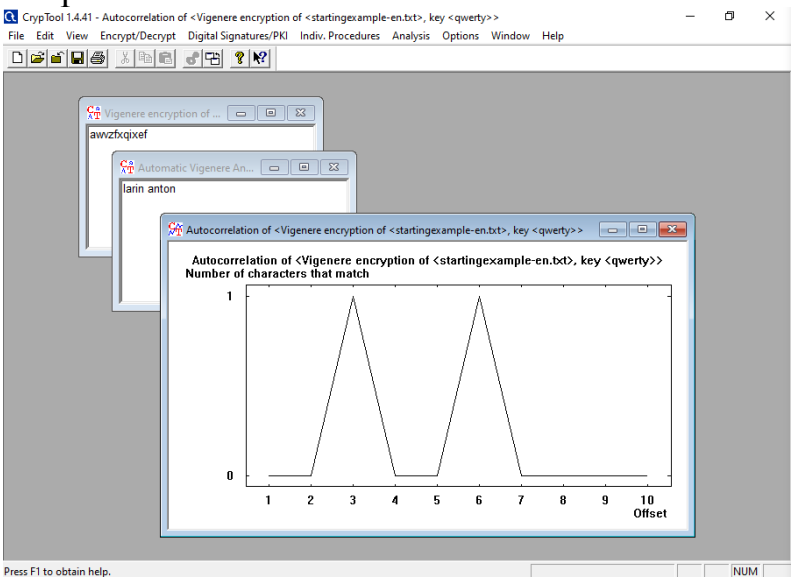


Рисунок 4. Анализ/атака на шифр виженера

5. Использован текст English.txt, взяты несколько параграфов. Получившийся текст зашифрован при помощи ключа qwerty и полного алфавита. Шифортекст и результат анализа представлены на рис. 5.

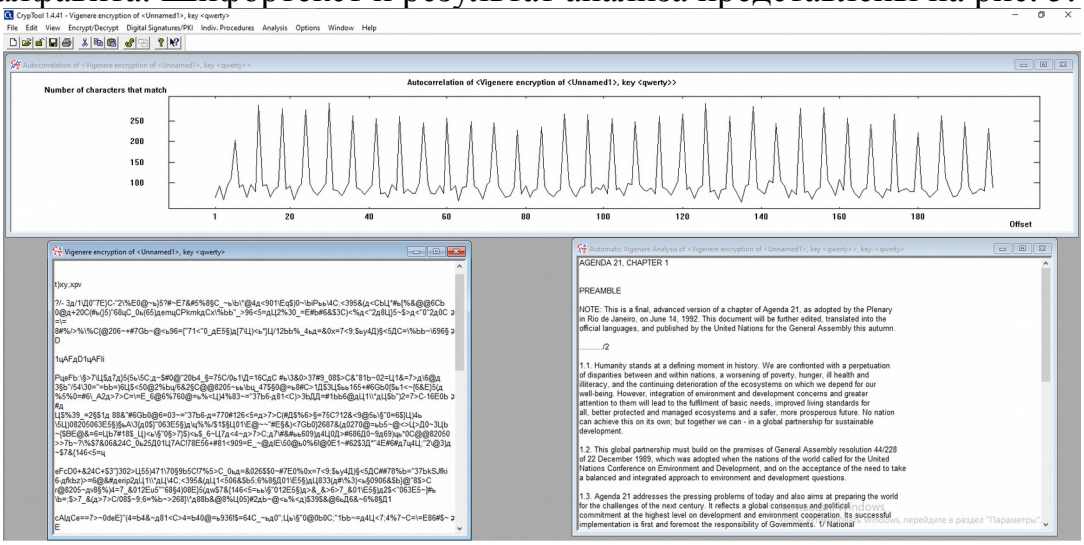


Рисунок 4. Анализ большого шифротекста виженера

6. Атака на шифротекст, зашифрованый шифром Виженера
Изучена атака на шифр Виженера реализованая в CrypTool2. Использован стандартный шифротекст
Результат представлен на рис. 5

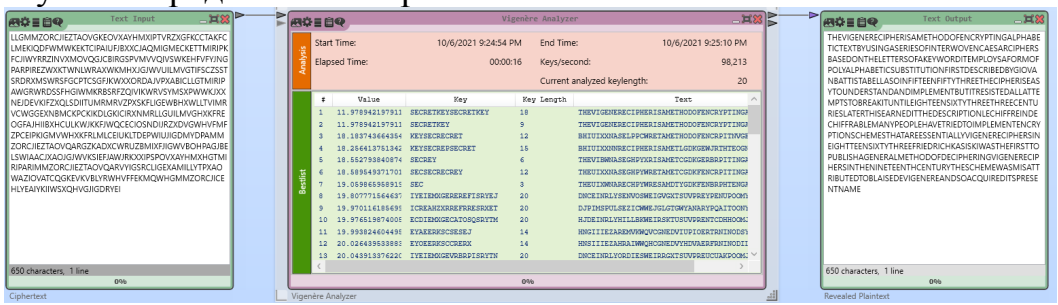


Рисунок 5. Анализ большого шифротекста виженера при помощи CrypTool2

Playfair

1. Шифровкм текста larin
   1. Разбтваем на пары символов
      la ri nx
   2. Составляем таблицу

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

   3. Получаем шифротекст
      qftgsc

4. Шифруем тот же текст. Получаем аналогичный результат. Он представлен на рис. 6.

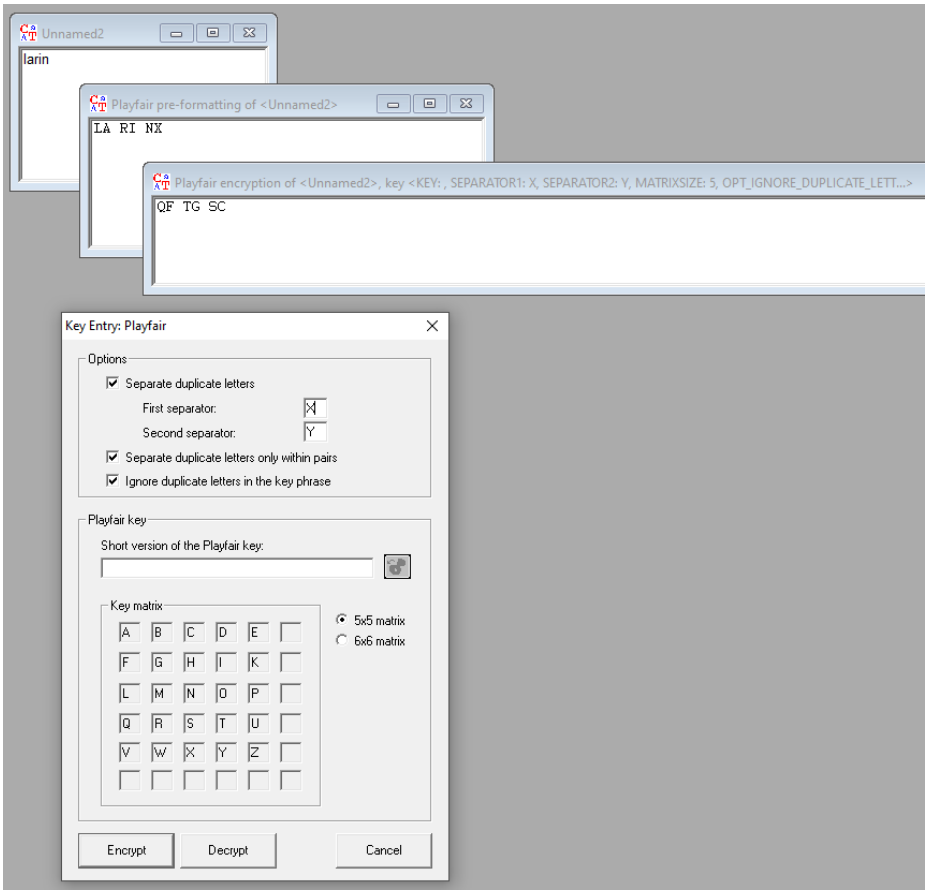


Рисунок 6. Шифровка при помщи шифра Playfair

2. Был взят текст «DEAR ALL THANK YOU FOR YOUR EFFORT» (Всем спасибо за старание)
    1. После шифрови получили шифротекст. Вид программы на рис. 7.
    EA BQ FQ OQ FC PH DT QK MT DT QS AK IL SU

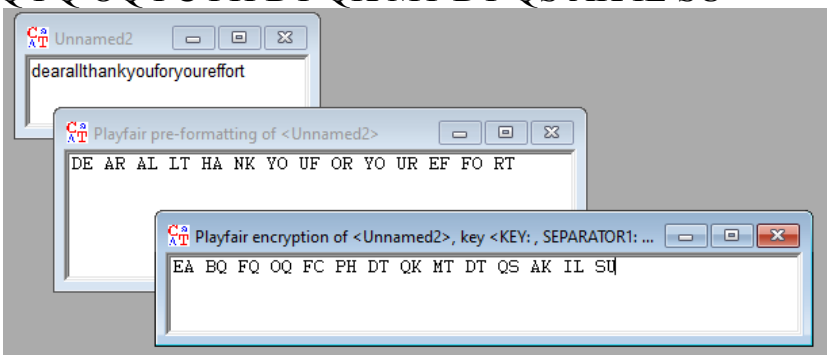


Рисунок 7. Шифровка при помщи шифра Playfair для последующей атаки

2. В инструмент анализа вписана известная часть. Вид на рис. 8.

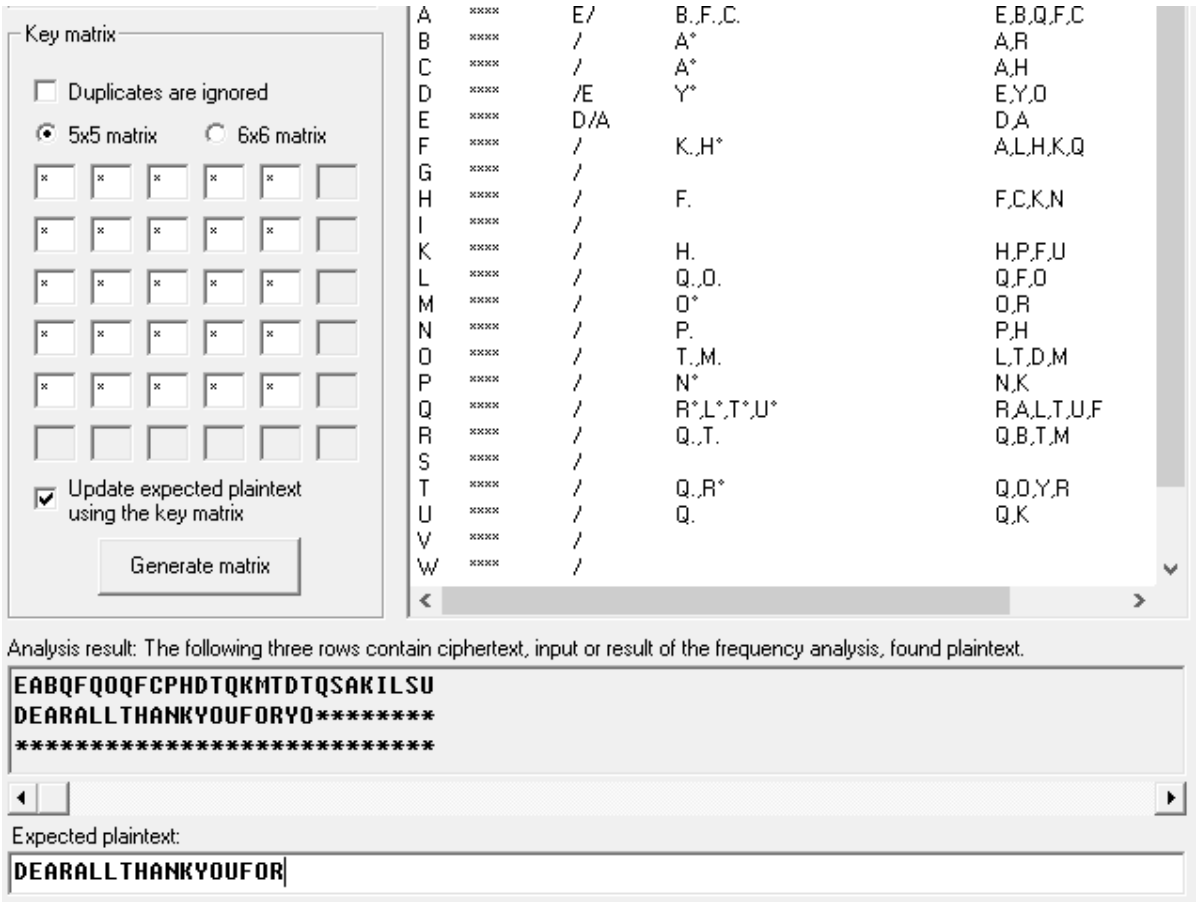


Рисунок 8. Первый шаг анализа Playfair по известной части

3. Восстановление части таблицы оп ручному анализу дает часть шифротекста. Она представлена на рис. 9

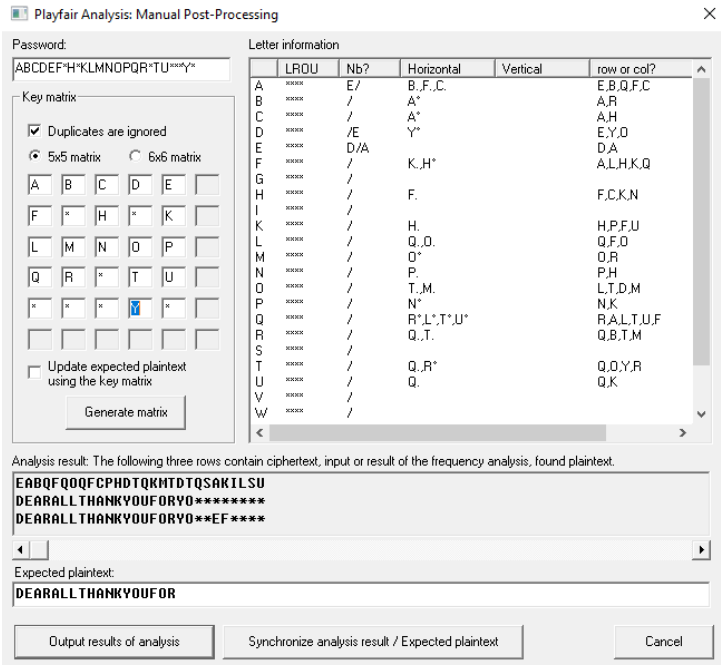
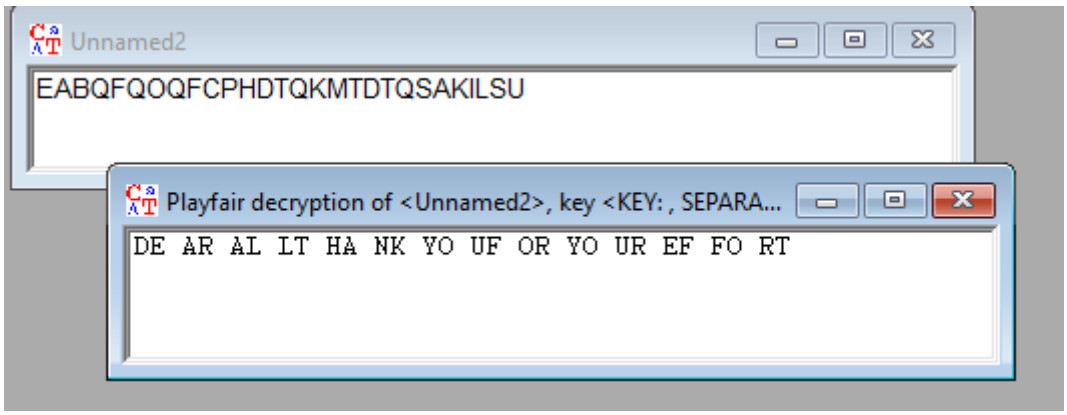


Рисунок 9. Часть восстановленного текста

4. Полная расшифровка выполнена корректно


Unnamed2
EABQFQOQFCPHDTQKMTDTQSAKILSU
Playfair decryption of <Unnamed2>, key <KEY: , SEPARA...
DE AR AL LT HA NK YO UF OR YO UR EF FO RT

Выводы.

Было исследовано три шифра - Сцитала, Виженера и Плейфера.

Для шифра сцитала исследован метод работы, влияние параметров числа граней и отступа на его работу. Исследование проведено на наборе цифр 0123456789 с двумя конфигурациями параметров (3;1) и (2;0). Также была проведена шифровка текста с фамилией - Larin. Результат работы Cryptool1 совпал с ручной зашифровкой во всех случаях.

Произведена атака на шифр при помощи грубой силы инструментом CrypTool2. Для этого использован стандартный темплейт, с заменой части с шифротекстом на блок с обычным текстом и блоком зашифровки. Если взять сложность расшифровки равной O(n), то сложность атаки на шифр равняется O(an), где a - Количество перебираемых параметров. В качестве текста для зашифровки был взят параграф из статьи, после чего атака грубой силой вернула искомsй текст, когда было найдено искомое число граней. При атаке искомое число было 11, проверка осуществлялась от 1 до 20.

Для шифра Виженера сначала был произведен эксперимент на зашивровки фамилии larin с ключем qwerty вручную и при помощи Cryptool1, получился шифротекст bwvzg в обоих случаях. Был произведен анализ инструментов autocorelation, результат которого показал длину ключа. То же было проделано с более длинным шифротекстом - несколькими параграфами из текста English.txt. Была произведена ручная атака на шифр при помощи перестановки текста длин Была произведена атака на шифр перестановкой с размером столбца равным размеру ключа.

Далее была проведена атака на шифр при помощи инструмента из CrypTool2. Она основана на оценке длины ключа и далее улучшения результатов при помощи методов оптимизации, т. е. последовательными приближениями на основе оценки изменения качества расшифровки.

Для шифра плейфера (Playfair), им была зашифрована фамилия larin с разбиением по парам символов и дополнением послежней пары символом X (la ri nx), ключем в виде квадрата 5*5 латинских символов в естественном порядке, что дало шифротекст qftgsc. Тот же результат был получем при помощи CrypTool1.

Далее был зашифрован текст с фиксированным началом "DEARALLTHANKYOUFORYOUREFFORT", он был разбит на пары (получилось без дополнений) и зашифрован. Получился шифротекст "EA BQ FQ OQ FC PH DT QK MT DT QS AK IL SU". На основе известной части была произведена полуручная атака с использованием CrypTool1. Анализ дал потенциальные символы, находящиеся рядом, на одной строке или в одном столбце. Эта информация была использована для восстановления полной матрицы, что позволило расшифровать исходный текст. Также была произведена атака при помощи инструмента CrypTool2, основанного на поиске наиболее вероятного исходного текста при помощи эвристических оценок результатов каждого подобранного ключа