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

ОТЧЕТ

по лабораторной работе №1-2-3
по дисциплине «Криптография и защита информации»
Тема: Изучение классических шифров
Rail Fence, Vigenere, Playfair

Студентка гр. 8383 _____ Гречко В.Д.

Преподаватель _____ Племянников А.К.

Санкт-Петербург
2021

Цель работы.

Исследовать шифры Rail Fence, Vigenere, Playfair и получить практические навыки работы с ними, в том числе с использованием приложений Cryptool 1 и 2.

Шифр Rail Fence.

Задание.

1. Найти шифр в CrypTool 1: Encrypt/Decrypt-> Symmetric(Classis).

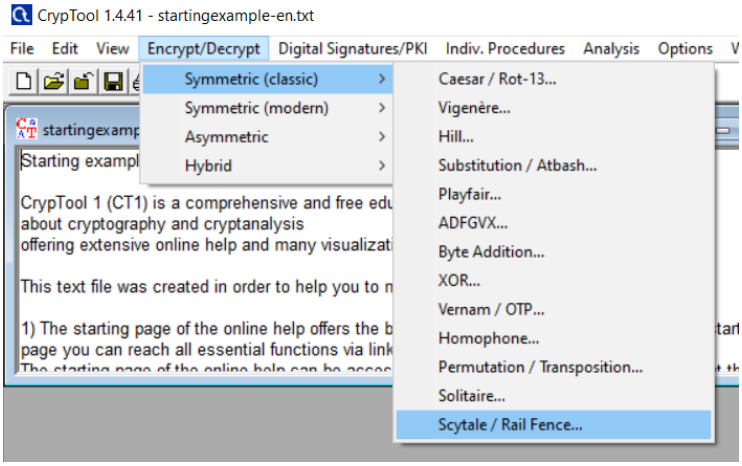


Рисунок 1 – Шифр Rail Fence в CrypTool 1

2. Создать файл с открытым текстом, содержащим последовательность цифр.

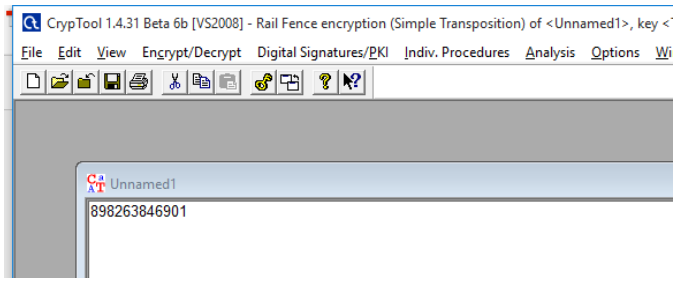


Рисунок 2 – Последовательность цифр

3. Запустить шифр и выполнить зашифровку и расшифровку созданного текста несколько раз.

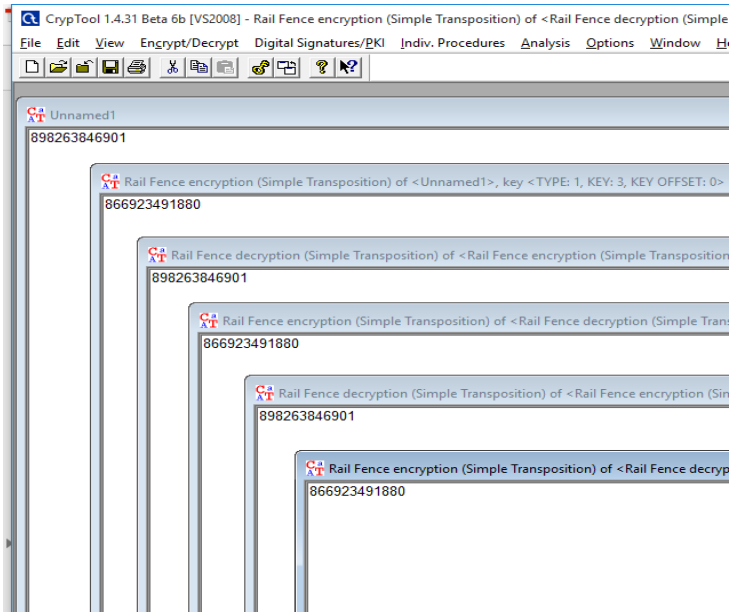


Рисунок 3 – Последовательность зашифровки и расшифровки

4. Установить, как влияют на шифрование параметры Number of Rows и Offset.

Number of Rows – количество строк в таблице шаблоне

Offset – смещение при записи открытого текста в шаблон

В общем случае данные параметры увеличивают криптостойкость шифра. Однако следует иметь в виду, что смещение стоит ставить от 0 до числа строк, так как в противном случае мы получаем идентичный результат.

5. Зашифровать и расшифровать текст, содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра при Number of Rows > 2, Offset ≥ 2. Убедиться в совпадении результатов.

Результат работы CrypTool 1:

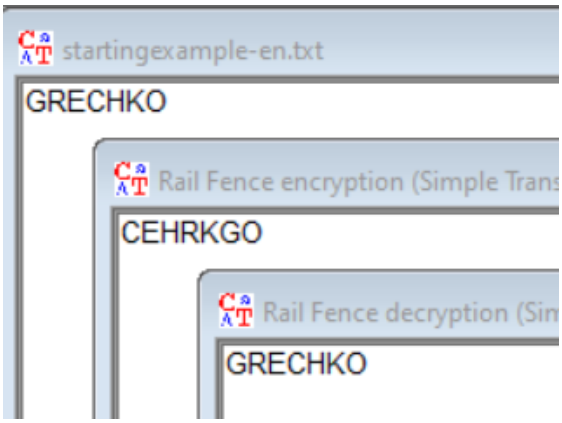


Рисунок 4 – результат работы программы

Результат ручной работы:

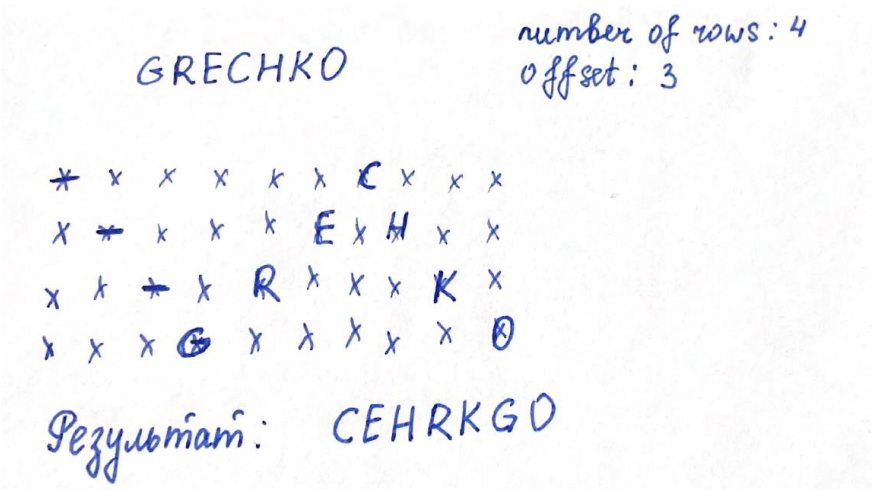
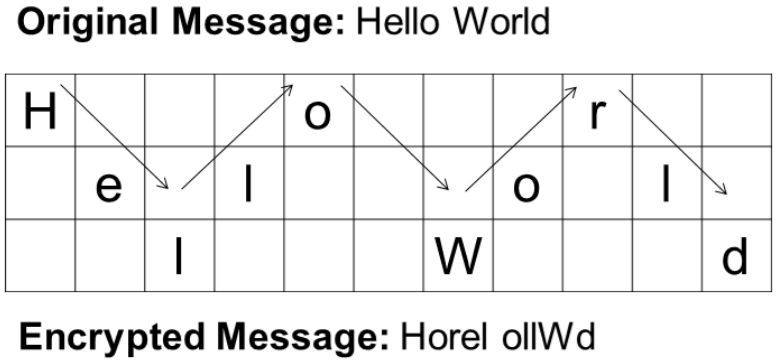


Рисунок 5 – результат ручного шифрования

Реализация в CrypTool 1.0 (скриншот, спецификация параметров):

В утилите CrypTool 1 присутствует возможность шифровки строки шифром Rail Fence. Text Options позволяет настроить допустимые символы для строки, а Number of Rows и Offset определяют ключ шифрования – отступ и число строк.

Схема, поясняющая работу шифра:



Пример работы шифра для выбранных параметров:

Строка	Number of Rows	Offset	Шифротекст
lavender	4	1	dlneaerv
	6	4	edrnelva
	7	2	larveedn

Тип шифра (перестановка, замена, комбинированный):

Перестановка

Ключ шифра:

Ключ шифра – это пара чисел, задающая число строк и смещение от начала таблицы-шаблона.

Оценка сложности атаки “грубой силы”:

$O(N \cdot (N-1))$, где N – размер входящего текста (число символов)

Результат расшифровки перехваченного от коллеги текста:

Ответ - NOTEBOOK

Шифр Vigenere

Задание.

1. Найти шифр в CrypTool 1: Encrypt/Decrypt-> Symmetric(Classic).

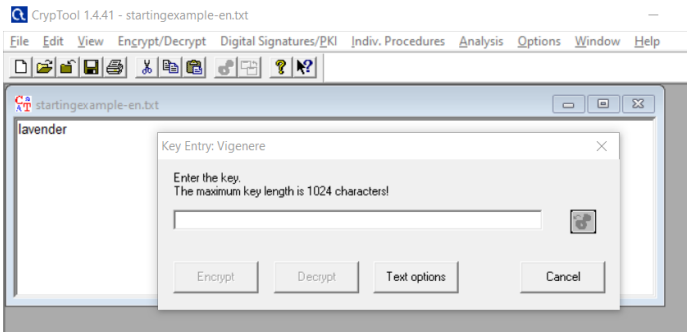
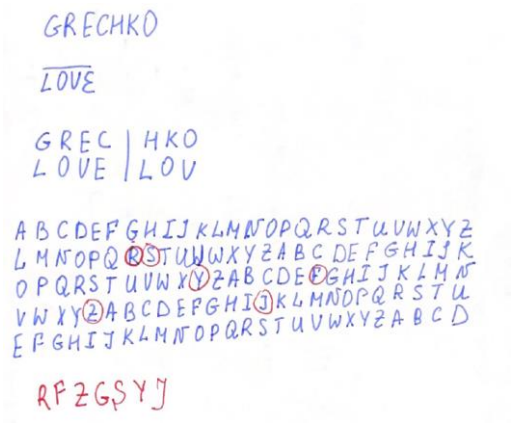


Рисунок 6 –Шифр Vigenere в CrypTool 1

2. Зашифровать и расшифровать текст, содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра с выбранным ключом. Убедиться в совпадении результатов.

Вручную:



С помощью программы:

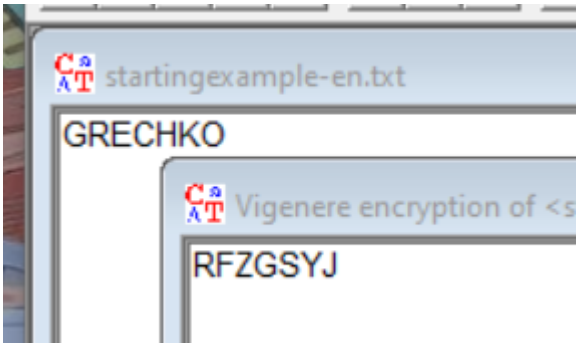


Рисунок 7 –Работа CrypTool 1

3. Произвести атаку на шифротекст, используя приложение *Analysis-> Symmetric Encryption(Classic)-> Cipher Text Only->Vigenere.*

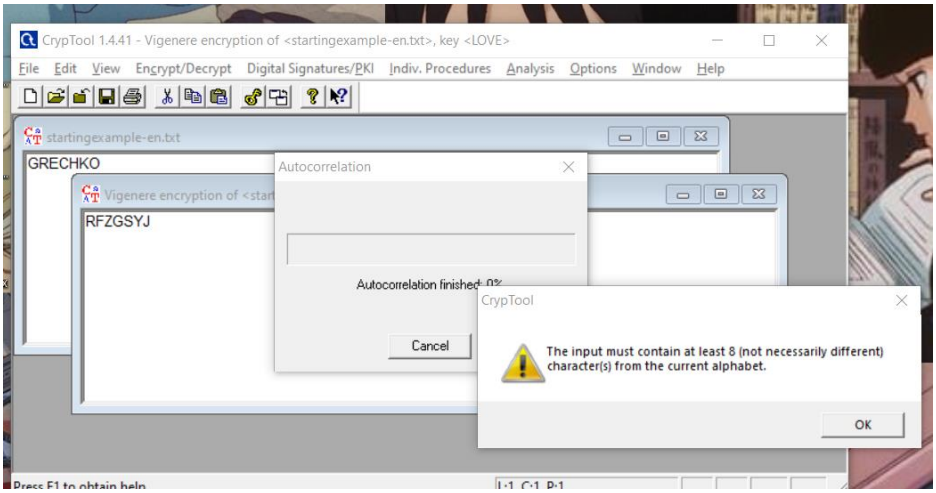


Рисунок 8 –Попытка расшифровки шифротекста CrypTool 1

Используем более длинное слово:

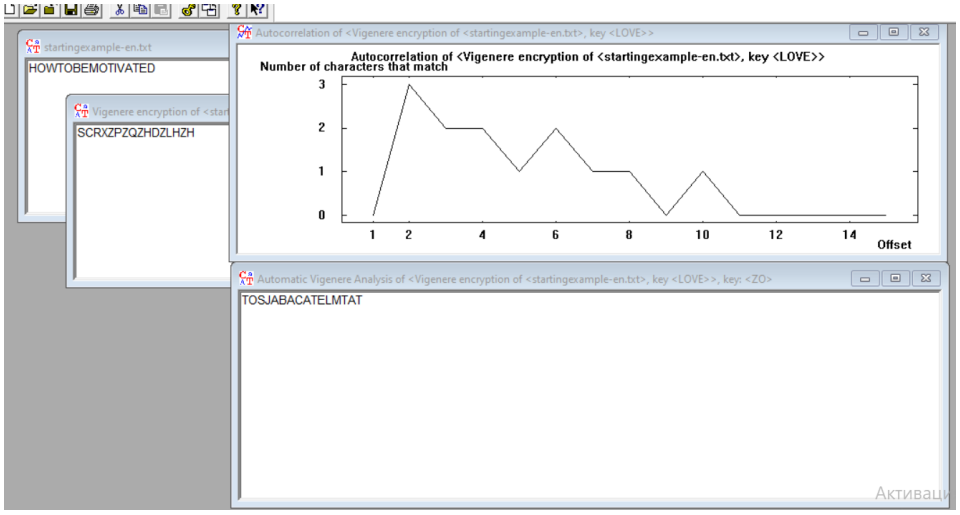
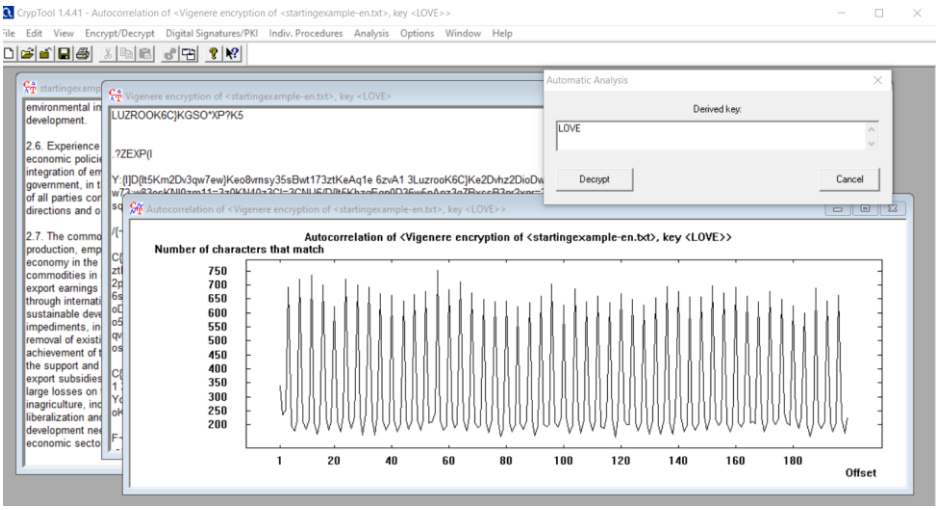


Рисунок 9 –Попытка расшифровки шифротекста CrypTool 1

4. Повторить атаку для фрагмента текста из файла English.txt (папка CrypTool/reference). Размер текста не менее 1000 символов.



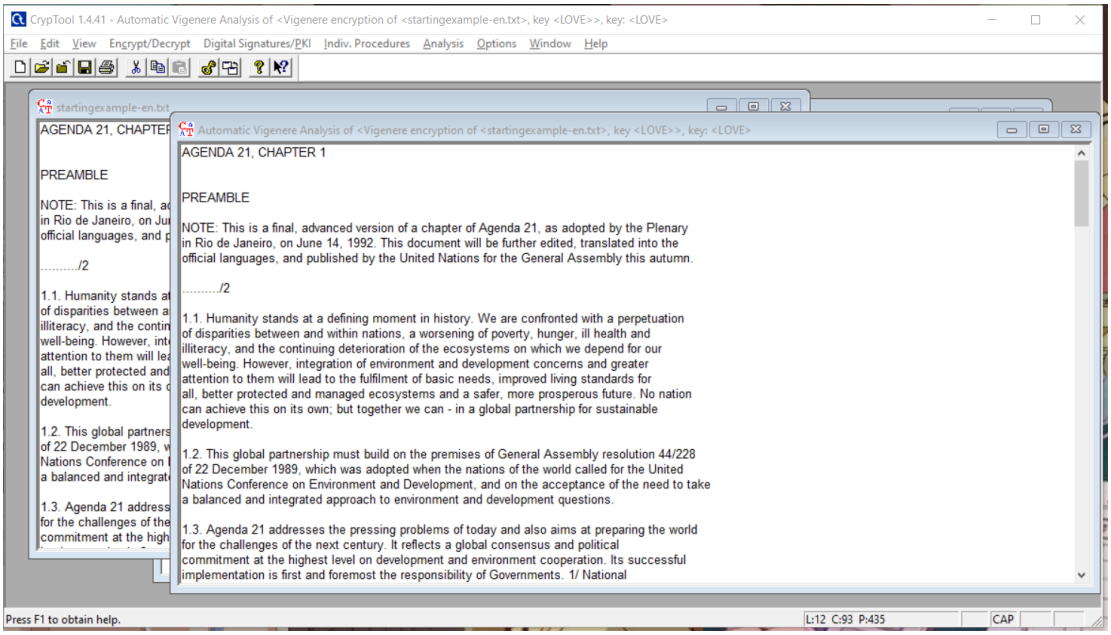
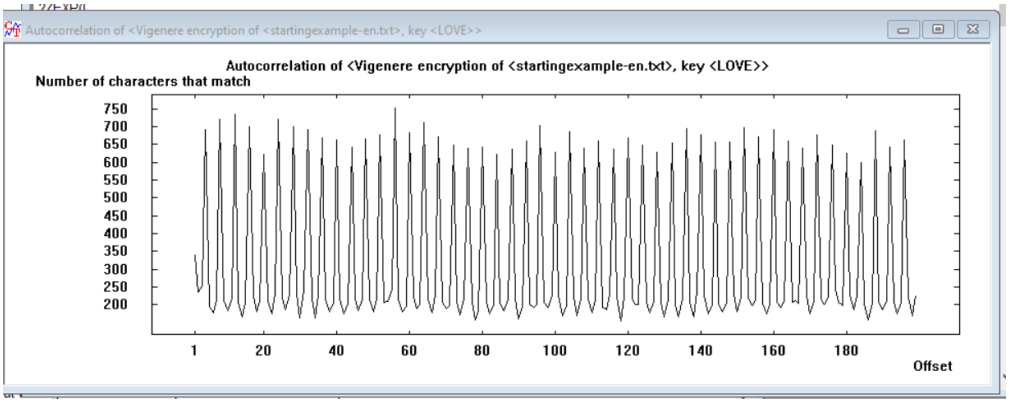
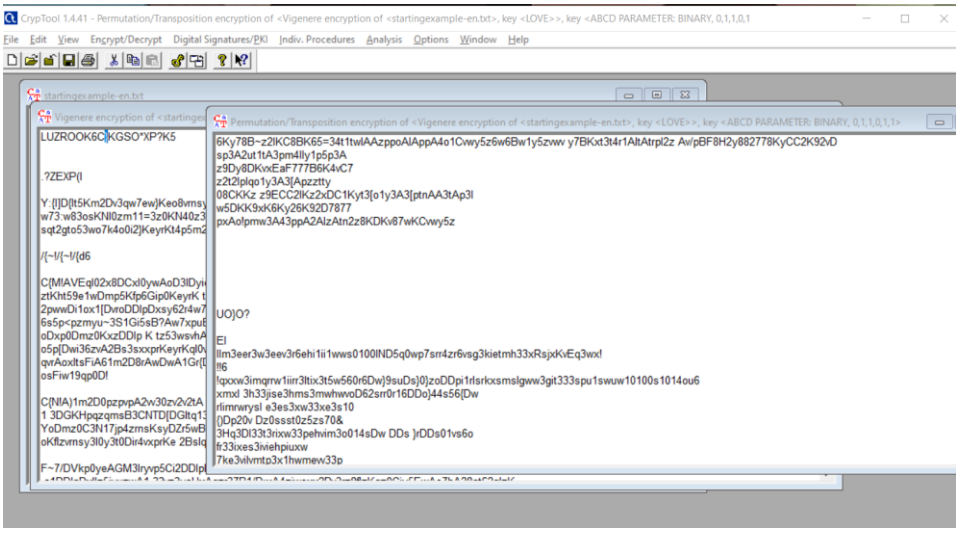


Рисунок 10 –Попытка успешной расшифровки шифротекста CrypTool 1

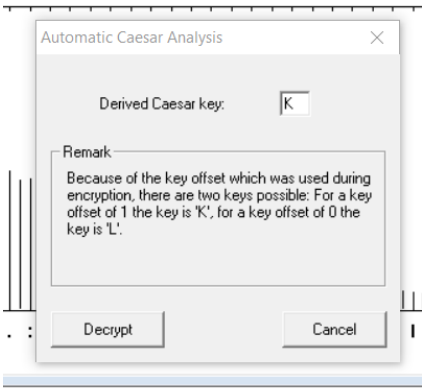
5. Воспроизведите эту атаку в автоматизированном режиме:
   a) Определите размер ключа с помощью приложения Analysis-> Tools for Analysis-> Autocorrelation

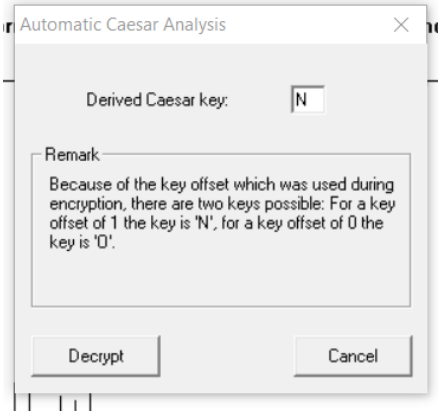


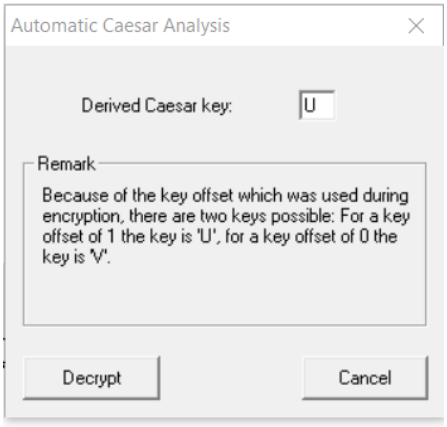
   b) Выполните перестановку текста с размером столбца равным размеру ключа приложением Permutation/Transposition

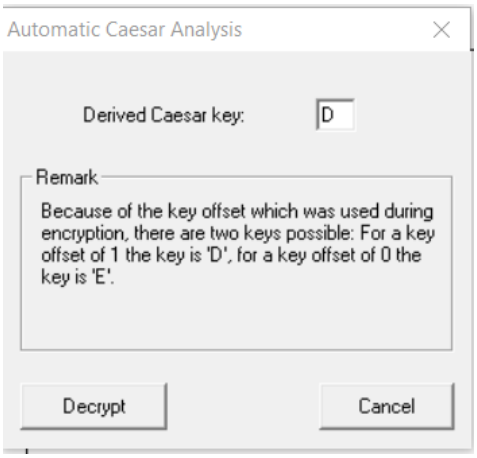


c) Определите очередную букву ключа приложением Analysis-> Symmetric Encryption(Classic)-> Cipher Text Only->Caesar.









6. Самостоятельно изучить атаку, реализованную в CrypTool 2, опираясь на Help и ссылки на статьи.

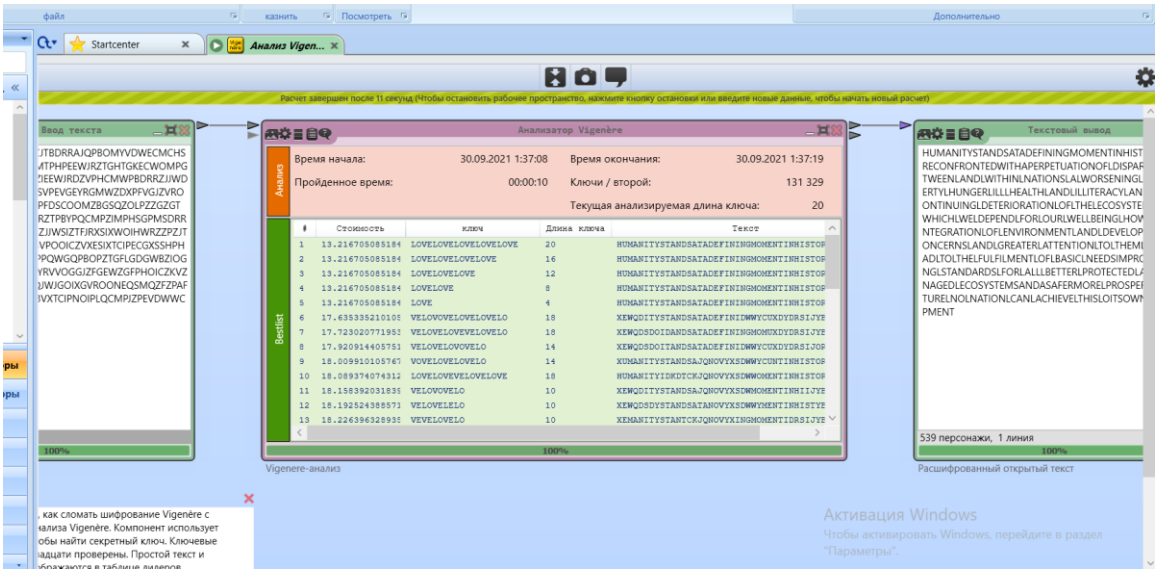
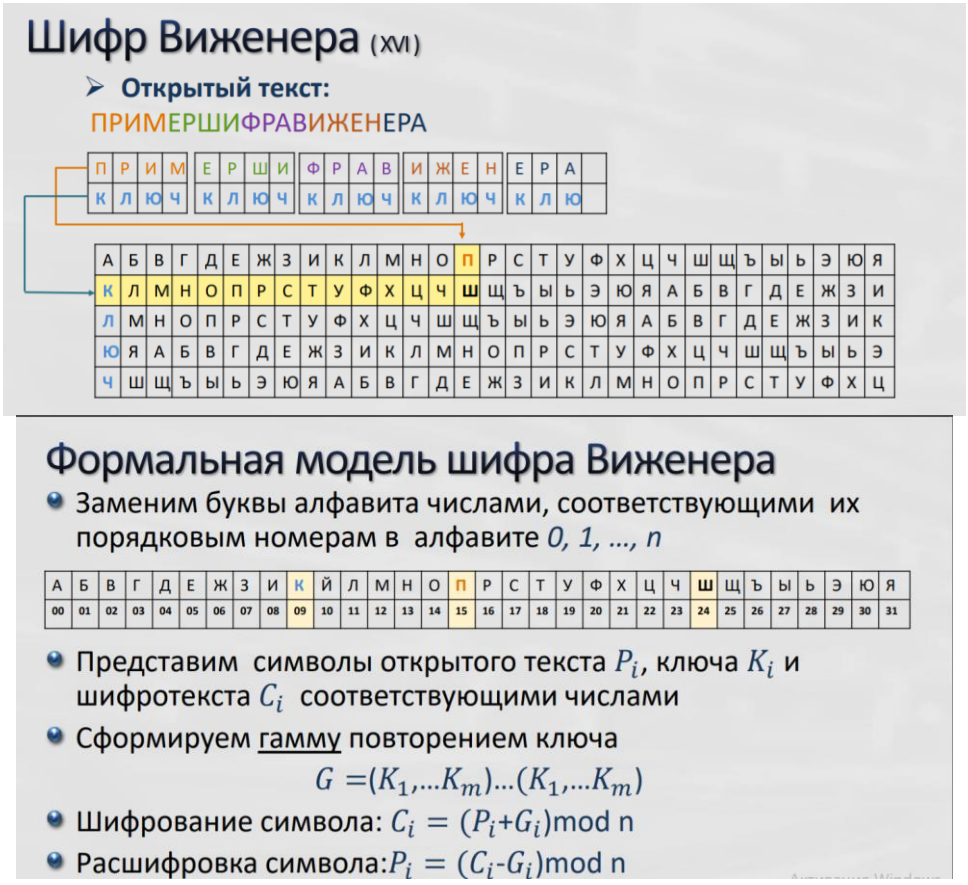


Схема и формулы, поясняющие работу шифра:



Пример работы шифра для выбранных параметров:

Строка	Ключ	Шифротекст
DEVELOPMENT	KEY	NITOPMZQCXX
	SUNSET	VYIWPHHGRFX
	ALLEY	DPGIJOAXILT

Тип шифра (перестановка, замена, комбинированный):

Замена

Ключ шифра:

Ключ шифра – это последовательность символов (ключевое слово).

Оценка сложности атаки “грубой силы”:

$\frac{n!}{(n-m)!}$, где n - размер алфавита, m – длинна ключа

Описание выполненной процедуры атаки на шифротекст и результат (ключ) этой атаки:

Сначала необходимо узнать длину ключа с помощью автокорреляционного метода. Далее с помощью статистического метода находят ключ. Для этого шифротекст разделяем на блоки одного алфавита. После этого применяем к каждому блоку анализ Caesar, узнаем возможный символ заданного алфавита

Описание атаки на шифр реализованной в CrypTool 2.0:

1) Первый шаг – выбирается случайный ключ, производится дешифровка с его использованием
2) Ключ изменяется, и для него рассчитывается “стоимость” – метрика, характеризующая полезность примененных изменений
3) Если изменение полезно, оно сохраняется, предпринимается дальнейшая попытка улучшить ключ
4) Шаги 2-3 повторяются до тех пор, пока ключ не станет нельзя улучшить

Шифр Плейфера (Playfair)

1. Исходное описание шифра (как в лекции).

Для работы алгоритма шифрования используется матрица 5*5 (но, если используется русский алфавит, то 4 * 8), в которую в произвольном порядке записываются символы алфавита. Этот я порядок можно задать кодовым словом. В этом случае, в первую строку записывается кодовое слово (без повторения символов) слева направо или по спирали из верхнего левого угла к

центру матрицы, а оставшиеся клетки матрицы заполняются незадействованными буквами алфавита в своем изначальном порядке.

Чтобы зашифровать текст его необходимо разбить на пары символов. 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.

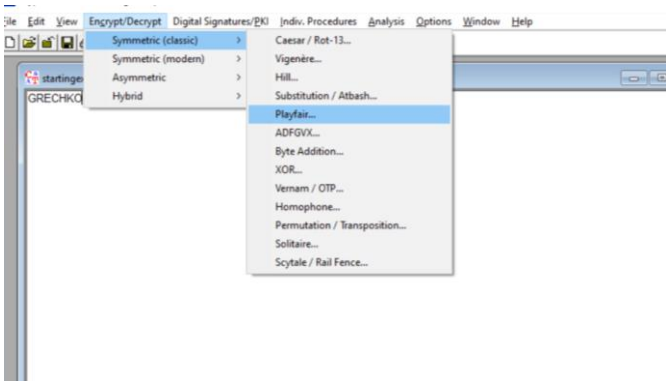
2. Если символы находятся в одной строке, то они замещаются на расположенные в ближайших от них справа символы.

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.

2. Реализация в Cryp Tool 1.0 (скриншот, спецификация параметров).



3. Пример работы шифра для выбранных параметров и текста сообщения.

Строка	Ключ	Шифротекст
GRECHKO	LOVE	DT OF IM VW
	SUNSET	LM ND IL PW
	YES	MX YD DN RU

4. Тип шифра (перестановка/замена/комбинированный, блочный/потоковый).

   Шифр Playfair является шифром типа “Замена”.

5. Ключ шифра.

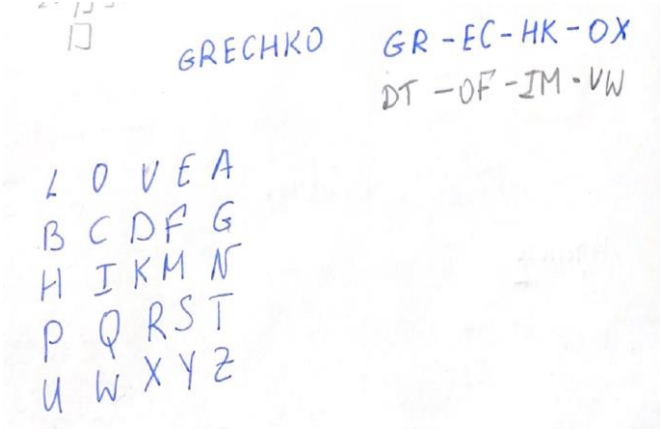
Ключом шифра является матрица $5 \cdot 5$ для латинского алфавита и $4 \cdot 8$ для кириллического

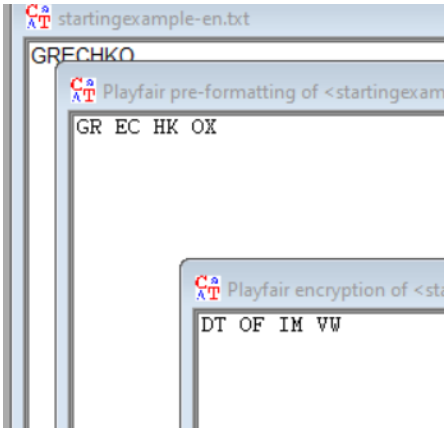
6. Оценка сложности атаки “грубой силы”.

При данной атаке придётся перебирать все возможные матрицы ключи – то есть $N!$, где N – мощность заданного алфавита

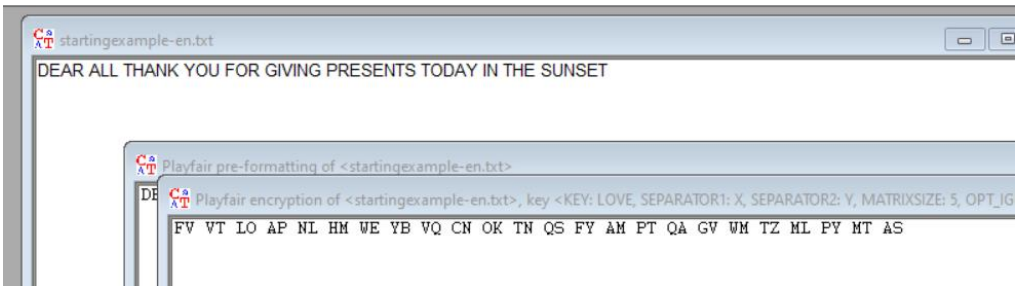
7. Описание методики атаки на шифр с использованием утилиты CrypTool 1.0.

7.1 Зашифровать и расшифровать текст, содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра с выбранной ключевой матрицей. Убедиться в совпадении результатов.



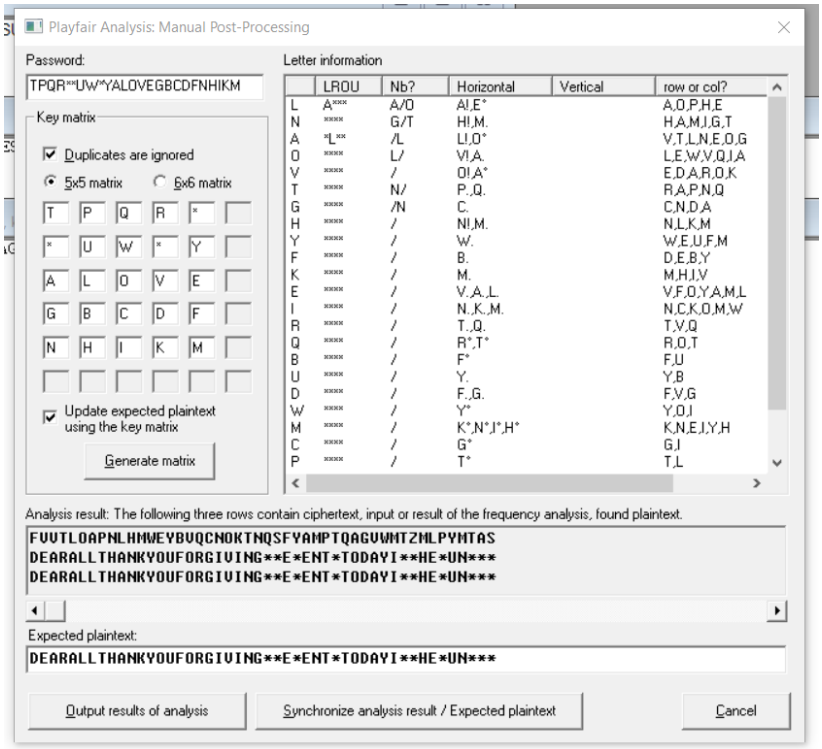


7.2 Зашифровать текст с произвольным сообщением в формате «DEAR ALL THANK YOU FOR ПРОИЗВОЛЬНЫЙ ТЕКСТ», используя выбранную шифрующую матрицу.



7.3 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



Выводы.

	Rail Fence	Vigenere	Playfair
Тип	Перестановка	Замена	Замена
Ключ	пара чисел, задающая число строк и смещение от начала таблицы-шаблона	последовательность символов (ключевое слово)	Матрица
Оценка сложности атаки “грубой силы”	$O(N \cdot (N-1))$, где N – размер входящего текста (число символов)	$\frac{n!}{(n-m)!}$	$O((n*m)!)$, где n и m – размеры ключ-матрицы
Описание	В каждую строку поочередно записывается одна буква со смещением, подобно изгороди.	Выбирается кодовое слово длины n, которое делит открытый текст на отрезки данной длины, составляется таблица Виженера. Элемент шифротекста выбирается на пересечении столбца, соответствующего букве открытого текста и строки, соответствующей букве кодового слова.	Замена биграмм через ключ-матрицу
Математическая формула	$x_i = (N \operatorname{div} n) \cdot \big((i \bmod n) - 1\big) + (i \operatorname{div} n)$	$c_j = \big(m_j + k_j\big) \bmod n$	-