**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**

|  |  |  |
| --- | --- | --- |
| Студент гр. 0303 |  | Болкунов В.О. |
| Преподаватель |  | Племянников А. К. |

Санкт-Петербург

2023

**Цель работы.**

Цель работы: исследовать шифры Rail Fence, Vigenere, ADFGVX и получить практические навыки работы с ними, в том числе с использованием приложений CrypTool 1 и 2.

**Порядок выполнения работы.**

1. Описать схему процесса зашифрования и расшифрования сообщения

2. Описать характеристики шифра: способ обработки символов сообщения (блочность), виды используемых операций над символами, определение ключа шифра в исследуемой реализации.

3. Произвести математический вывод оценки асимптотической сложности атаки "грубой силы"

4.  Выполнить и описать атаку на шифровку.

**Выполнение работы.**

**1. Шифр «Изгородь» (Rail Fence)**

**1.1. Процесс зашифрования**

В данном шифре исходное сообщение вписывается по диагонали в таблицу с заданной высотой (высота изгороди). Зашифрованный текст получается путём конкатенации символов в одной строке и объединением всех строк, например для сообщения на рисунке 1, вписанного в таблицу высотой **3**, шифротекст будет следующим: «0481357926»

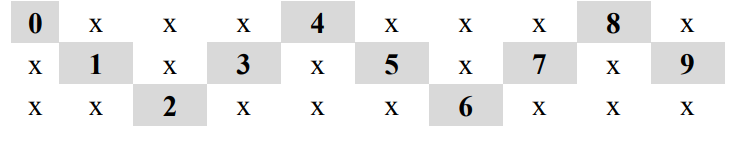


Рисунок 1: шифр изгородь без смещения

Для расшифрования необходимо поместить сообщение в исходную таблицу и провести действия в обратном порядке.

В общем случае для увеличения криптостойкости шифр изгороди может иметь сдвиг (рис. 2).

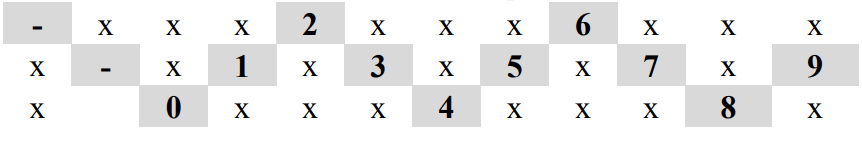


Рисунок 2: шифр изгородь со сдвигом 2

Процесс шифрования и расшифрования аналогичен случаю без сдвига, пропущенные символы не учитываются. Для примера на рисунке 2 шифротекст будет следующим: «2613579048»

С помощью программы Cryptool 1 было выполнено шифрование и расшифрование текста, состоящего из цифр данным шифром, результаты представлены на рисунке 3.

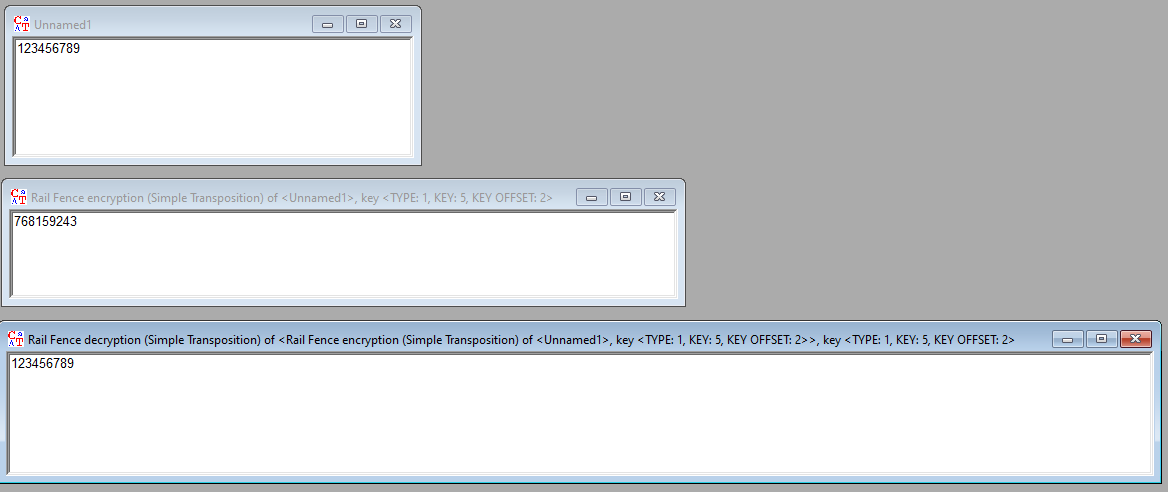


Рисунок 3: Cryptool шифр изгородь

**1.2. Характеристики шифра**

Шифр является перестановочным, ключом для него служит пара чисел , соответственно высота изгороди и сдвиг. Для процесса шифрования используется всё сообщение, целиком записанное в таблицу, соответственно шифрование и расшифрование нельзя производить поблочно.

**1.3. Оценка сложности атаки**

Для атаки грубой силой необходимо перебрать возможные ключи, а именно пары возможные пары высоты изгороди и сдвига - . Высота изгороди очевидно должна быть меньше длины сообщения и больше единицы, чтобы шифротекст отличался от исходного сообщения. На сдвиг же можно наложить следующие ограничения: , так как длина пути из верхней точки изгороди до нижней и наоборот будет , итого для создания «периода» (смещение 0 будет идентично смещению ). Итого , где n *–* размер сообщения

Тогда количество операций перебора ключа будет следующим:

Итого асимптотическая сложность атаки составляет .

**1.4. Атака на шифровку**

Так как шифр является перестановочным, единственным способом атаки является перебор ключей до тех пор, пока не получится осмысленное сообщение. На рисунке 4 изображён пример подбора ключа для сообщения «Do not go gentle into that good night». Выделенное сообщение является дешифровкой с правильно подобранным ключом.

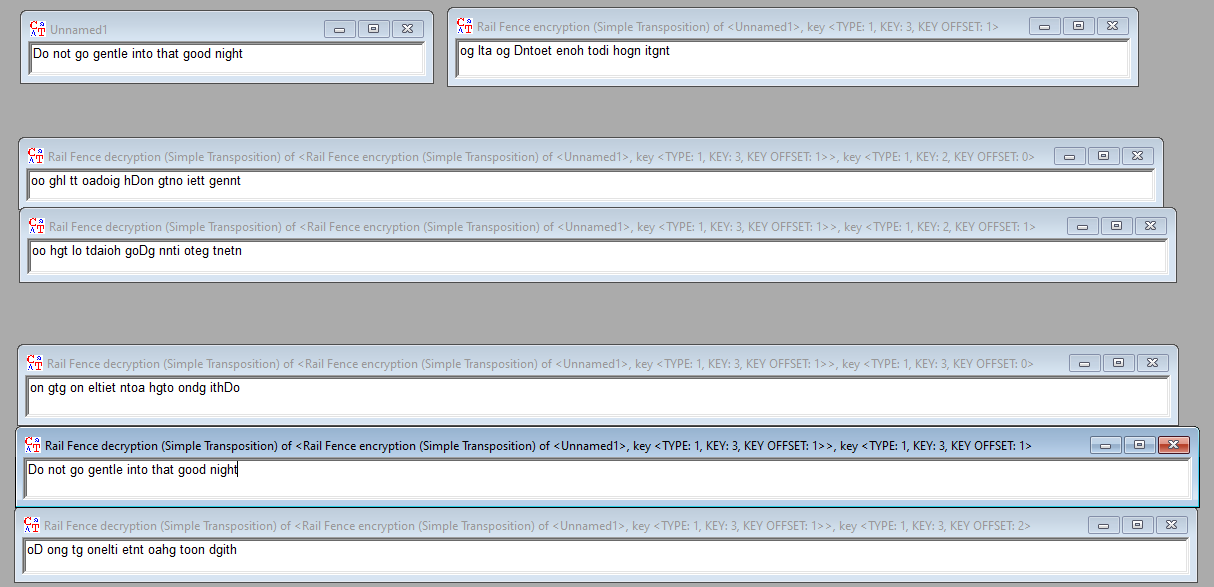


Рисунок 4: атака на шифр изгороди

**2. Шифр Виженера**

**2.1. Процесс зашифрования**

Для шифрования сообщения используется таблица замен, построенная с помощью выбранного ключа. Первой строкой таблицы записывается алфавит, а первым столбцом – ключ. Далее каждая строка дополняется символами, идущими после символа ключа в текущей строке (циклично). Например, для слова ключа «ключ» таблица будет следующей:



Рисунок 5: таблица виженера для слова "ключ"

После создания таблицы исходный текст разбивается на блоки размером равным размеру ключа, в каждом блоке сопоставляются символы сообщения и символы ключа и на их пересечении в таблице выбирается символ, который будет записан в шифротекст.

Пример шифрования с помощью ключа «ключ» текста «примершифравиженера» изображён на рисунке 6.

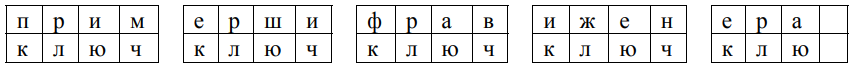


Рисунок 6: пример шифра виженера

Для расшифровки сообщение аналогично разбивается на фрагменты, но при замене символа выбирается символ первой строки, находящийся в столбце, в котором находится текущий символ сообщения в строке текущего символа ключа.

С помощью программы Cryptool 2 было проведено шифрование и расшифрование текста с помощью шифра Виженера. Результаты представлены на рисунке 7.

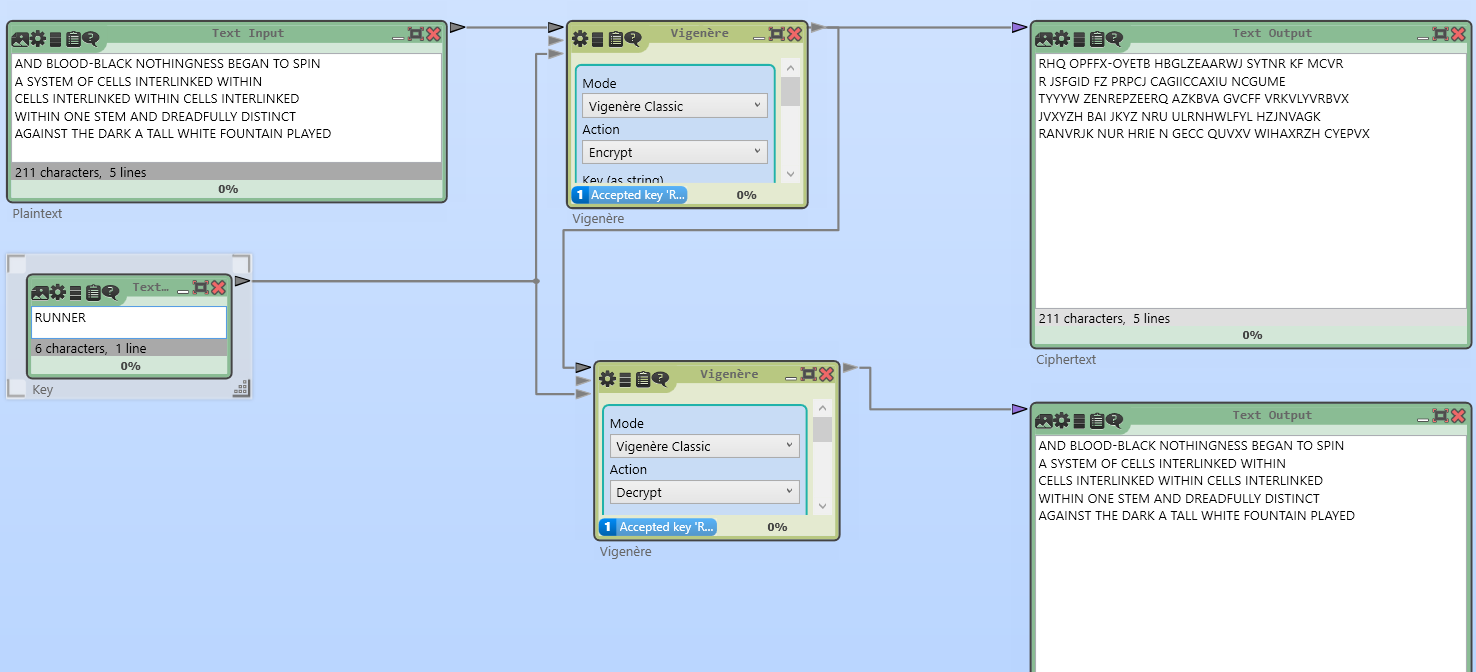


Рисунок 7: шифр Виженера

**2.2. Характеристики шифра**

Шифр Виженера является шифром многоалфавитной замены, ключом для него служит выбранное слово, состоящее из символов алфавита сообщения. Шифровку и расшифровку можно осуществлять имея блок с размером ключа, то есть шифр блочный.

**2.3. Оценка сложности атаки**

Для атаки грубой силы необходимо перебрать все возможные ключи (размер ключа ограничен размером исходного текста, так как следующие символы ключа будут отброшены), и все возможные комбинации символов в ключах:

где n – размер сообщения, k – размер ключа на очередной итерации атаки и *A* – размер алфавита. Что асимптотически приближается к для латинского алфавита. Естественно, что за адекватное время методом грубой силы ключ подобрать невозможно.

Однако используя перебор в совокупности с частотным анализом можно подобрать сначала размер ключа, а затем и символы в ключе. Если предположить, что частотный анализ можно сделать за ***n*** операций, то асимптотическая сложность такой гибридной атаки будет:

**2.4. Атака на шифровку**

С помощью средств криптоанализа Cryptool 2 была проведена атака на шифр Виженера (рис. 8), полученная дешифровка идентична исходному сообщению (без учёта пробелов)

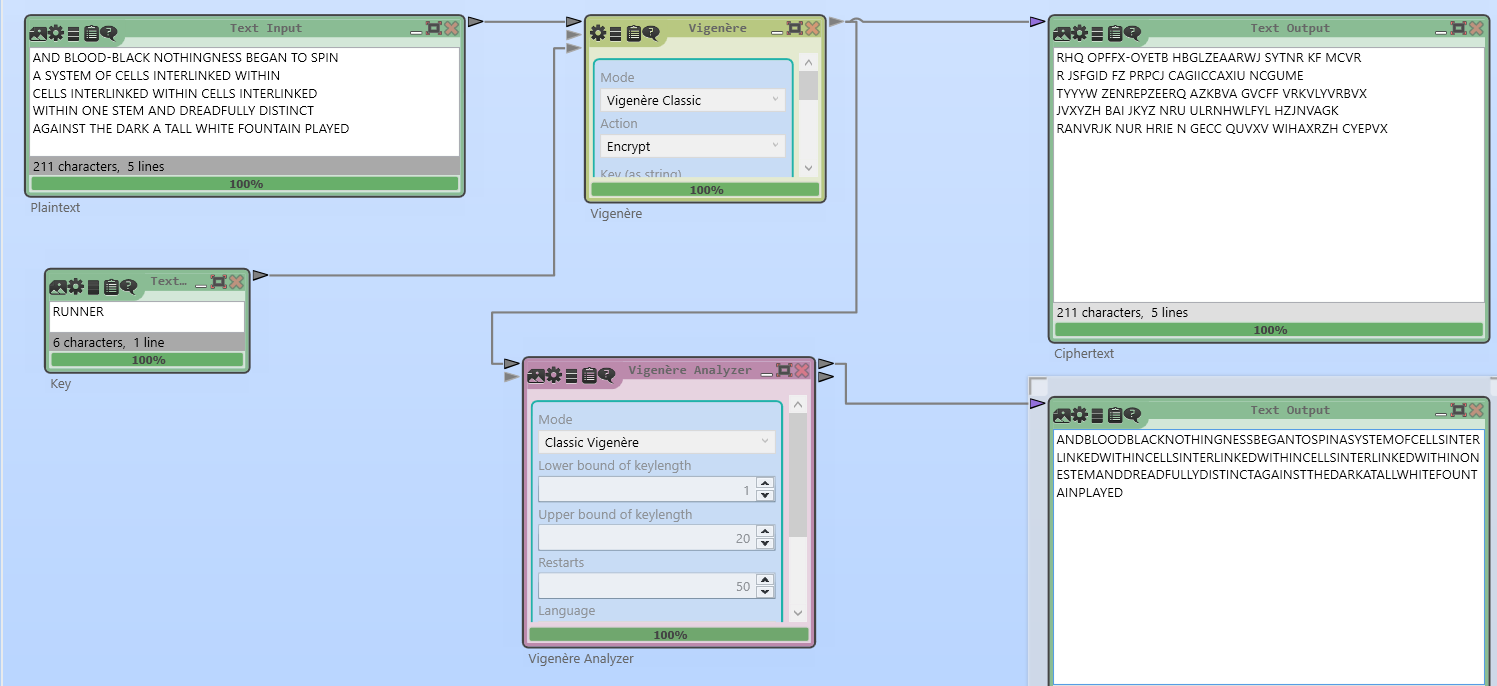


Рисунок 8: атака на шифр Виженера

**3. Шифр ADFGVX**

**3.1. Процесс зашифрования**

На первом этапе шифрования заполняется матрица для шифрования индексируемая символами и построенная с помощью **ключа замены**: из ключа убираются повторяющиеся символы, и он записывается построчно в таблицу, оставшиеся символы дописываются по порядку. Например, для ключа замены «147REGIMENT» матрица шифрования будет следующая:

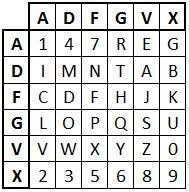


Рисунок 9: матрица для шифрования ADFGVX

Далее каждый символ сообщения кодируется парой индексов (*ADFGVX*), которые записываются в матрицу шириной равной размеру **ключа перестановки**. И в конце столбцы полученной матрицы перемешиваются в соответствии с порядком символов в ключе перестановки (символы ключа становятся по порядку в алфавите, а вместе с ними перемещаются и столбцы матрицы). Например, для ключа «OURKEY» перестановка будет следующая:

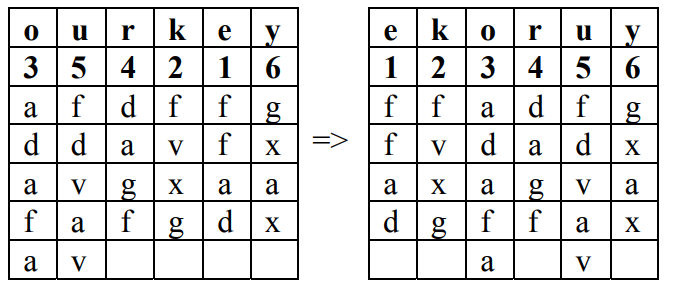


Рисунок 10: перестановка в ADFGVX

Для расшифровки действия производятся в обратном порядке: переставляются столбцы матрицы сообщения и производится замена биграм на символы в шифрующей матрице.

С помощью программы Cryptool 2 было осуществлено шифрование и расшифрование сообщения данным шифром. Результаты изображены на рисунке 11.

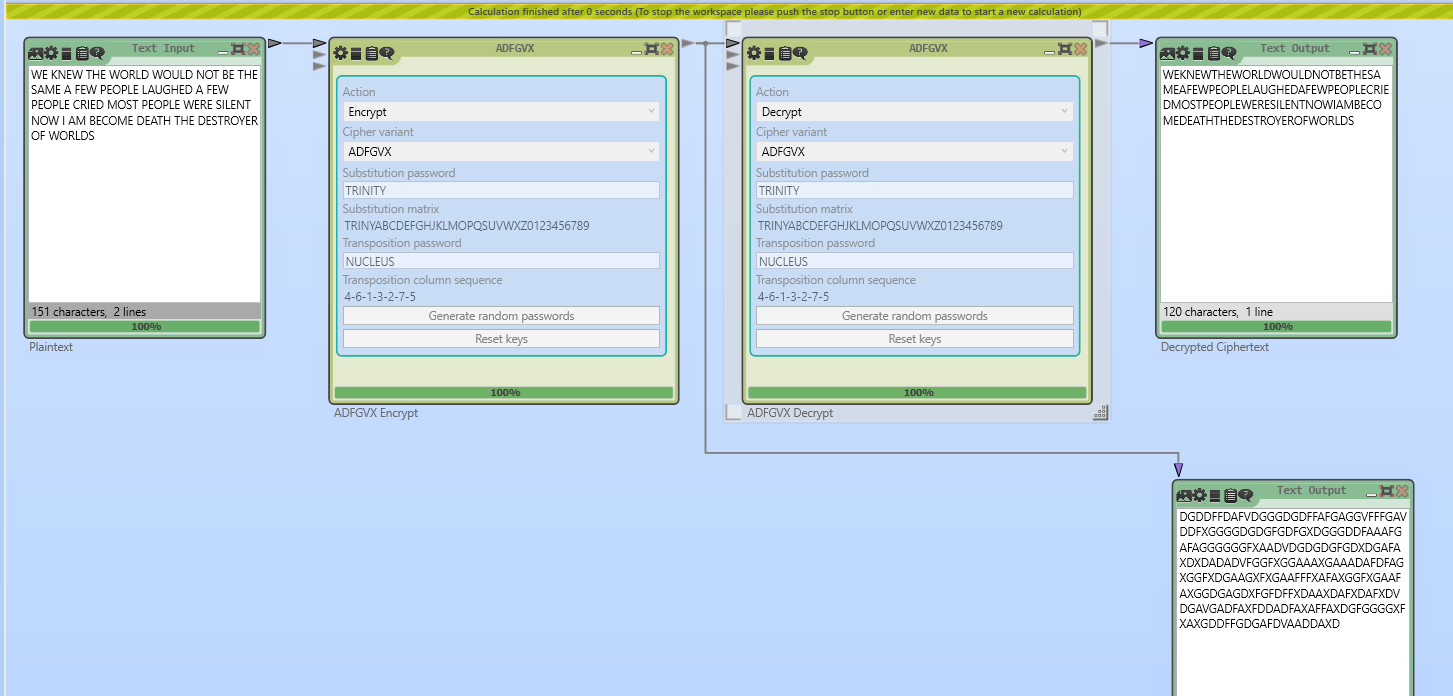


Рисунок 11: ADFGVX

**3.2. Характеристики шифра**

Шифр ADFGVX производит как замену, так и перестановку. Он не блочный, так как осуществляет перестановку, для которой необходимо иметь весь исходный текст или шифротекст.

**3.3. Оценка сложности атаки**

Для атаки грубой силы необходимо перебрать возможные длины ключа замены: от 1 (отсутствие перестановки) до размера сообщения ***n*** (переставлена каждая буква). Далее необходимо перебирать сами перестановки – на каждом шаге . И после этого перебирать матрицу замены -

Итого: . Значение значительно превосходит **,** что значит что сложность более сложная чем факториальная, что делает атаку грубой силой бессмысленной при анализе достаточно больших сообщений.

**3.4. Атака на шифровку**

С помощью программы Cryptool 2 и последовательного соединения анализаторов ADFGVX и моноалфавитной замены была произведена атака на данный шифр, для ускорения работы ключи были упрощены. Анализатор ADFGVX реализует некий эвристический алгоритм, способный найти ключ перестановки, но не даёт информации о ключе замены, далее так как одни и те же символы шифруются одинаковыми биграммами возможно провести частотный анализ с помощью анализатора моноалфавитной замены.

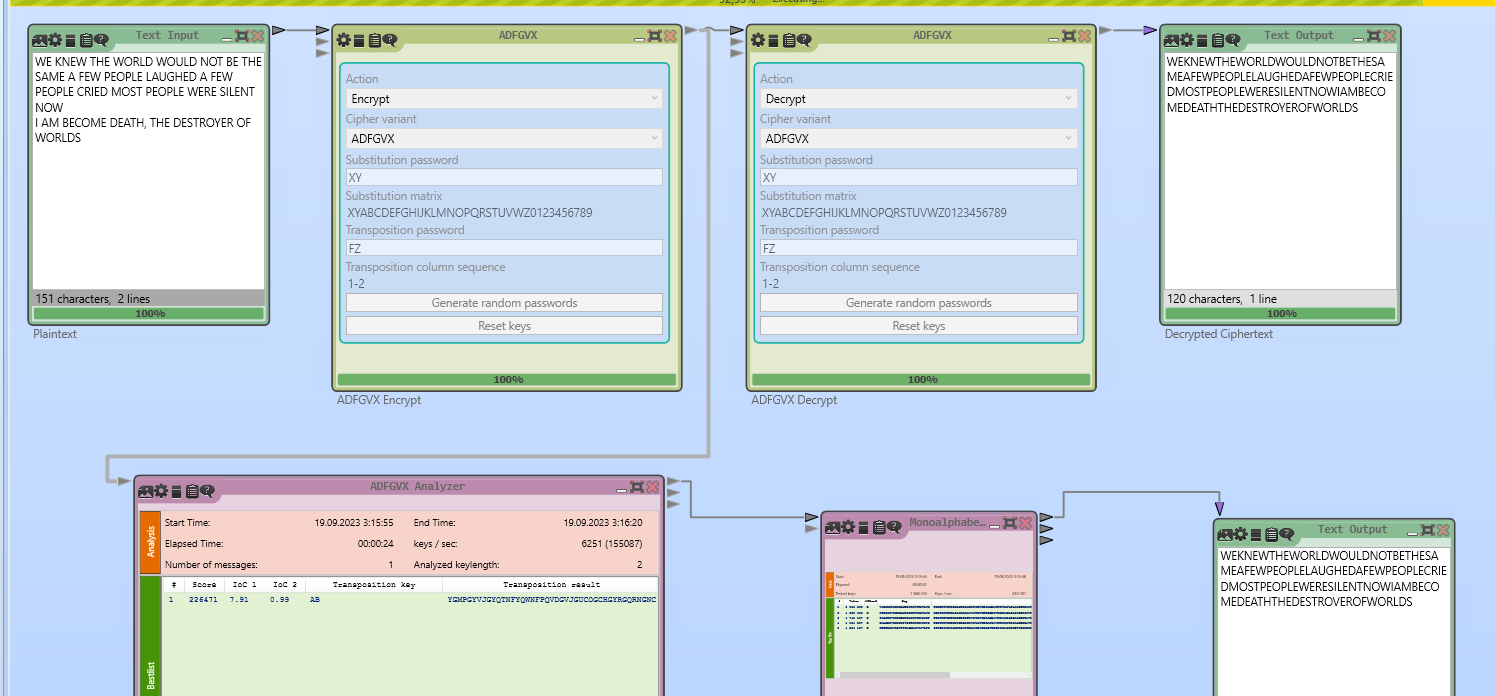


Рисунок 12: атака на ADFGVX

**Выводы:**

В ходе выполнения работы были исследованы классические шифры:

* Изгородь (Rail Fence)
* Шифр Виженера
* ADFGVX

Для каждого из шифров:

* был исследован и описан процесс шифрования и расшифрования сообщений,
* с помощью средств Cryptool 1 и 2 были реализованы шифрование и расшифрование сообщений с заданным ключом,
* исследованы характеристики шифра,
* выведена математическая оценка сложности атаки грубой силы
* и проведена атака на шифровку с помощью средств Cryptool 1/2.