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»

0	x	x	x	**4**	x	x	x	**8**	x
x	**1**	x	**3**	x	**5**	x	**7**	x	**9**
x	x	**2**	x	x	x	**6**	x	x	x

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).

-	x	x	x	2	x	x	x	6	x	x	x
x	-	x	1	x	3	x	5	x	7	x	9
x		0	x	x	x	4	x	x	x	8	x

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.

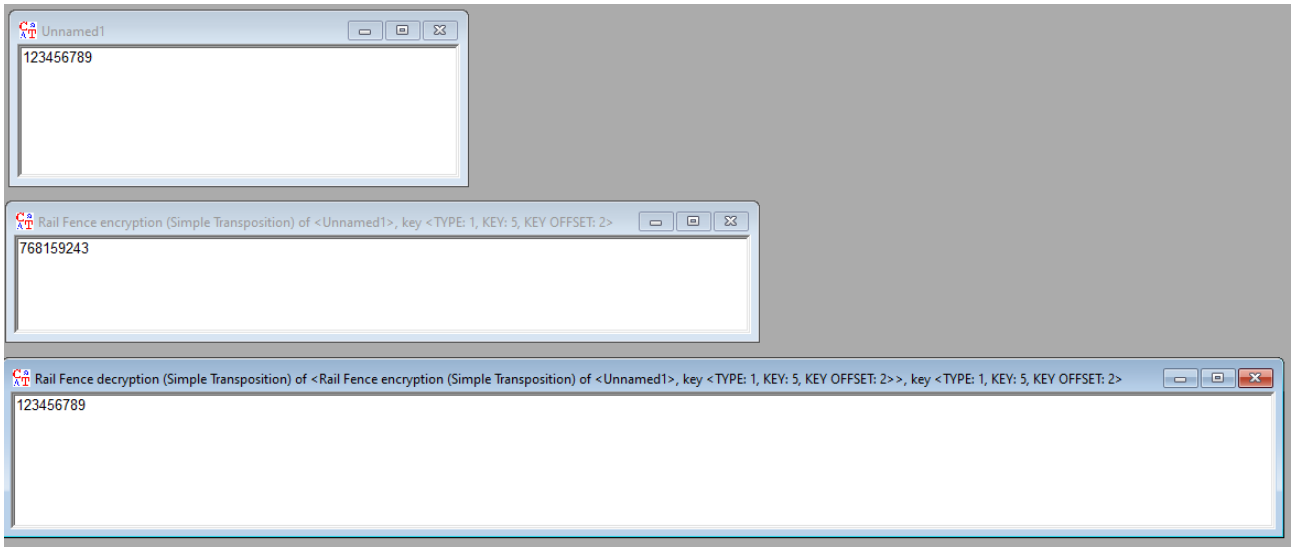

Рисунок 3: Cryptool шифр изгородь

1.2. Характеристики шифра

Шифр является перестановочным, ключом для него служит пара чисел (k, m), 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 - (k, m). Высота изгороди очевидно должна быть меньше длины сообщения и больше единицы, чтобы шифротекст отличался от исходного сообщения. На сдвиг же можно наложить следующие ограничения: $[0; 2k - 3]$, так как длина пути из верхней точки изгороди до нижней и наоборот будет $k - 1$, итого $2k - 2$ для создания «периода» (смещение 0 будет идентично смещению $2k - 2$). Итого $m \in [0; 2k - 3], k \in [2; n - 1]$, где n – размер сообщения

Тогда количество операций перебора ключа будет следующим:

$$O(n) = \sum_{k=2}^{n-1} \sum_{m=0}^{2k-3} 1 = (n-1)n \approx \boldsymbol{n^2}$$

Итого асимптотическая сложность атаки составляет n^2.

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 $(3, 1)$ для сообщения «Do not go gentle into that good night». Выделенное сообщение является дешифровкой с правильно подобранным ключом.

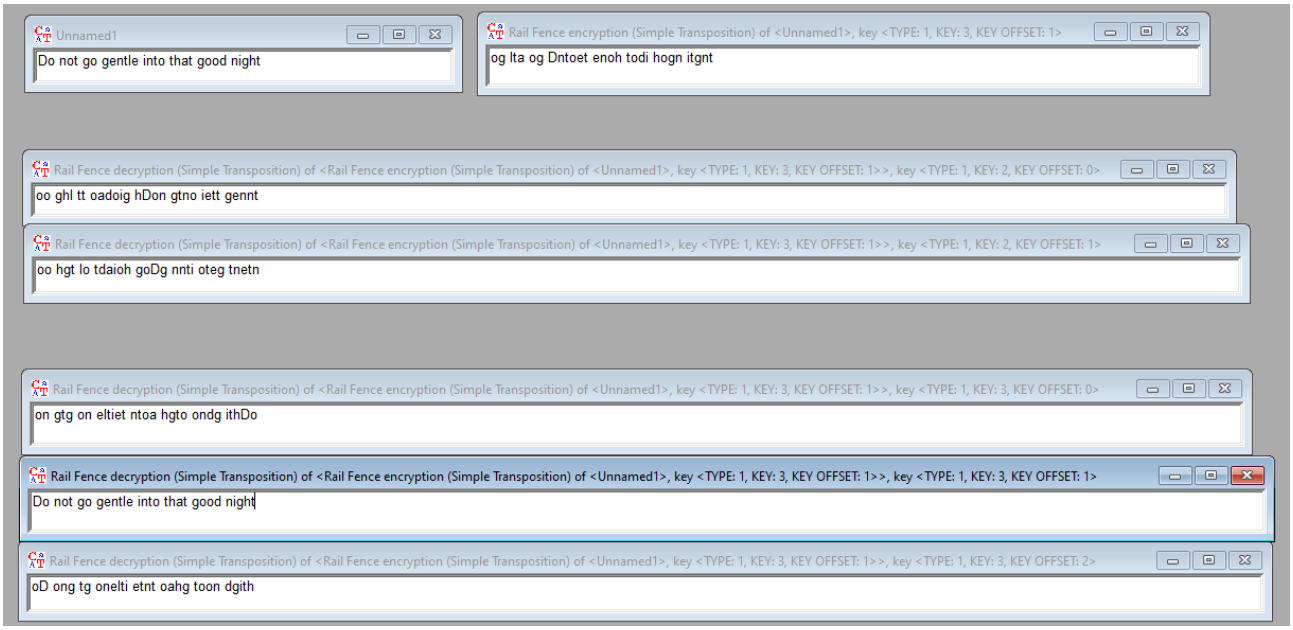

Рисунок 4: атака на шифр изгороди

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:

а	б	в	г	д	е	ж	з	**и**	к	л	**м**	н	о	**п**	**р**	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
К	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	**ш**	**щ**	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и
Л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	**ъ**	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	к
Ю	я	а	б	в	г	д	е	**ж**	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
Ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	**в**	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц

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.

п	р	и	м
к	л	ю	ч

е	р	ш	и
к	л	ю	ч

ф	р	а	в
к	л	ю	ч

и	ж	е	н
к	л	ю	ч

е	р	а	
к	л	ю	

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.

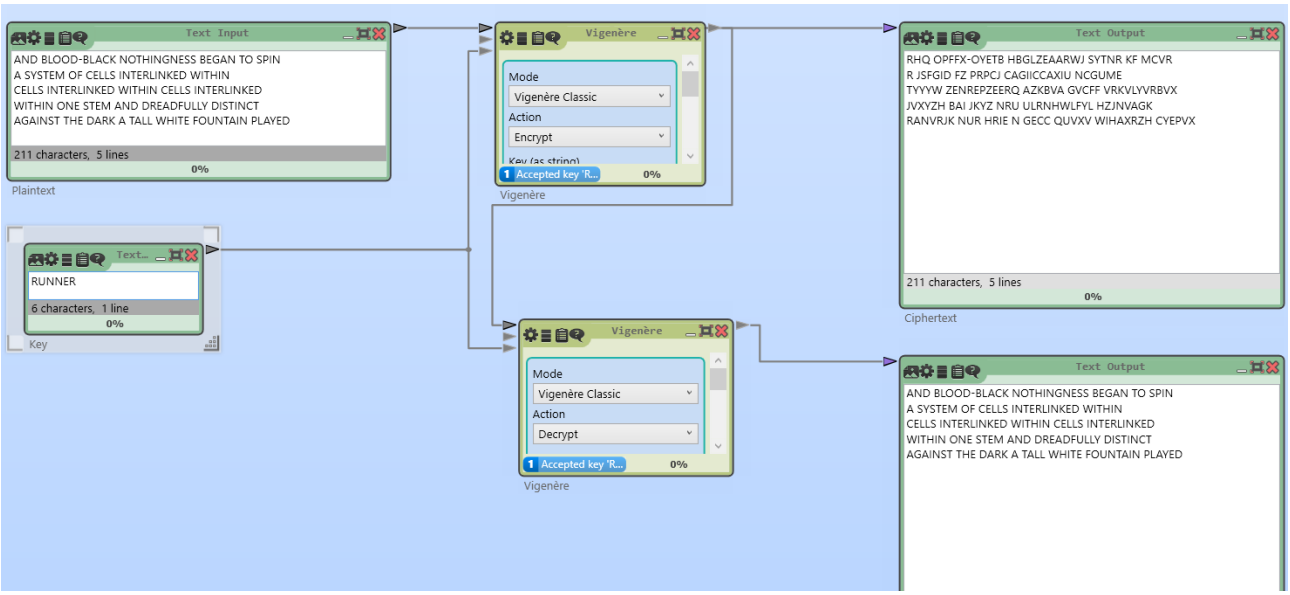

Рисунок 7: шифр Виженера

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:

$$O(n) = \sum_{k=1}^{n} A^n$$

где n – размер сообщения, k – размер ключа на очередной итерации атаки и A – размер алфавита. Что асимптотически приближается к $\boldsymbol{26^n}$ 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 $\boldsymbol{n}$ операций, то асимптотическая сложность такой гибридной атаки будет: $O(n) \approx n^2$

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)

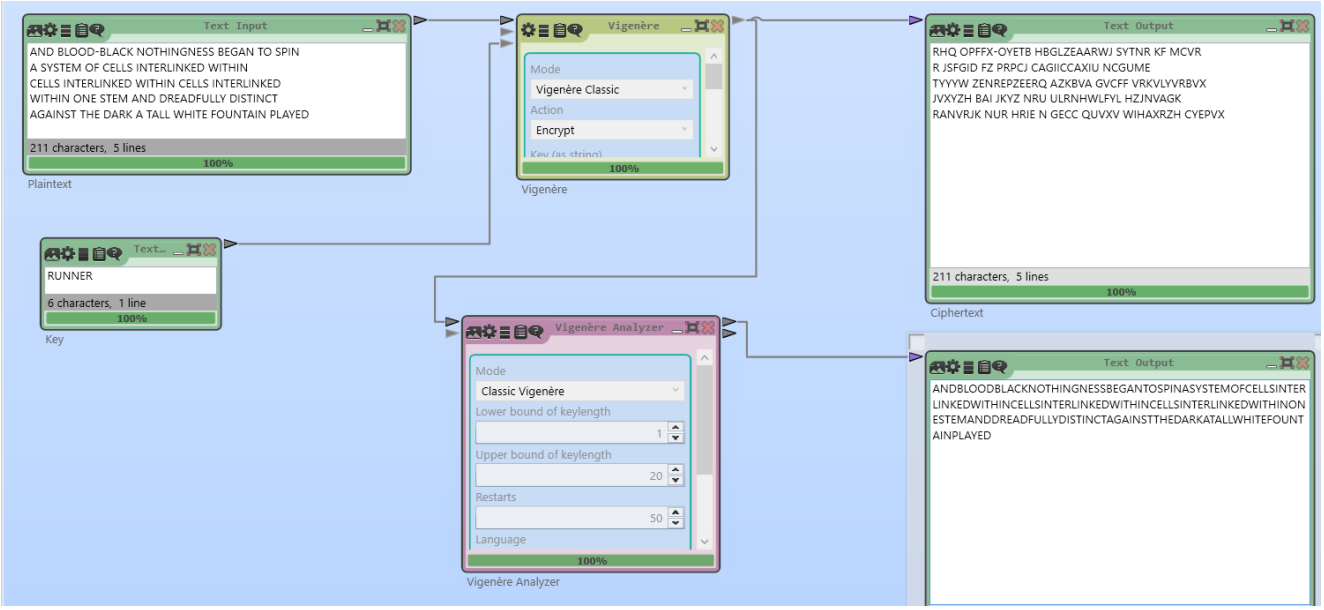

Рисунок 8: атака на шифр Виженера

3. Шифр ADFGVX

3.1. Процесс зашифрования

На первом этапе шифрования заполняется матрица для шифрования (6×6) индексируемая символами A, D, F, G, V, X 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:

	A	D	F	G	V	X
A	1	4	7	R	E	G
D	I	M	N	T	A	B
F	C	D	F	H	J	K
G	L	O	P	Q	S	U
V	V	W	X	Y	Z	0
X	2	3	5	6	8	9

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:

o	u	r	k	e	y
3	5	4	2	1	6
a	f	d	f	f	g
d	d	a	v	f	x
a	v	g	x	a	a
f	a	f	g	d	x
a	v				

=>

e	k	o	r	u	y
1	2	3	4	5	6
f	f	a	d	f	g
f	v	d	a	d	x
a	x	a	g	v	a
d	g	f	f	a	x
		a		v	

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.

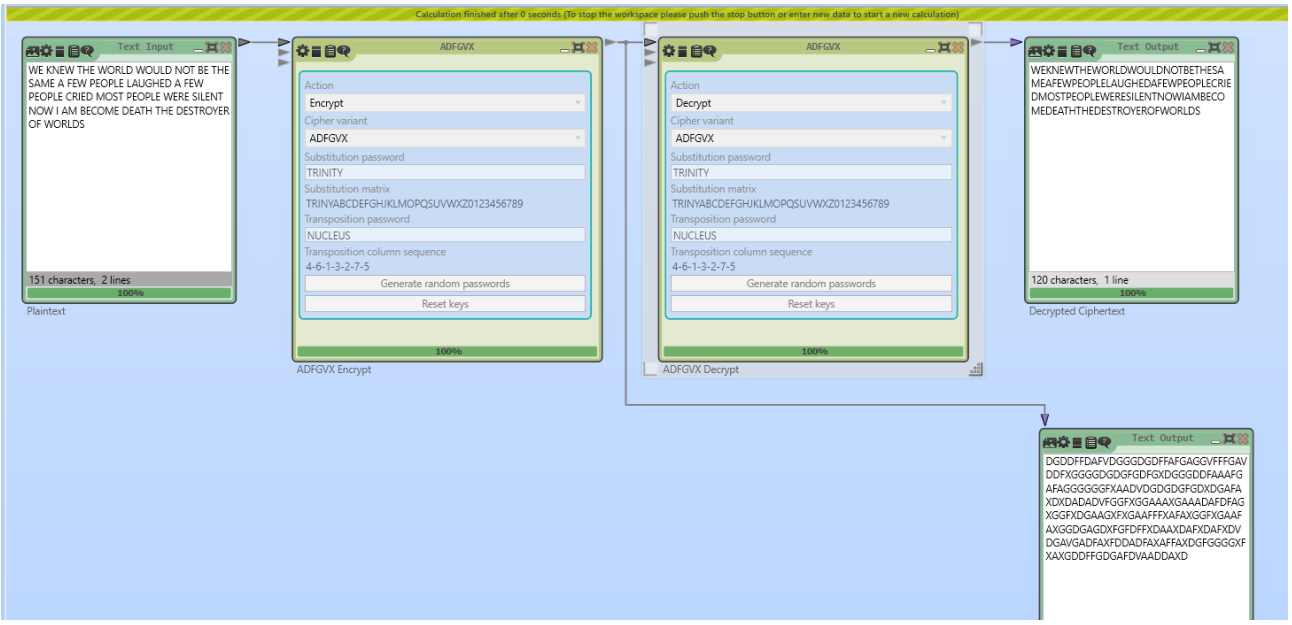

Рисунок 11: ADFGVX

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 $\boldsymbol{n}$ (переставлена каждая буква). Далее необходимо перебирать сами перестановки – на каждом шаге $\boldsymbol{k}!$. И после этого перебирать матрицу замены - $36!$

Итого: $O(n) = \sum_{k=1}^{n} k! * 36!$. Значение значительно превосходит $\boldsymbol{36!\, n!}$, 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.

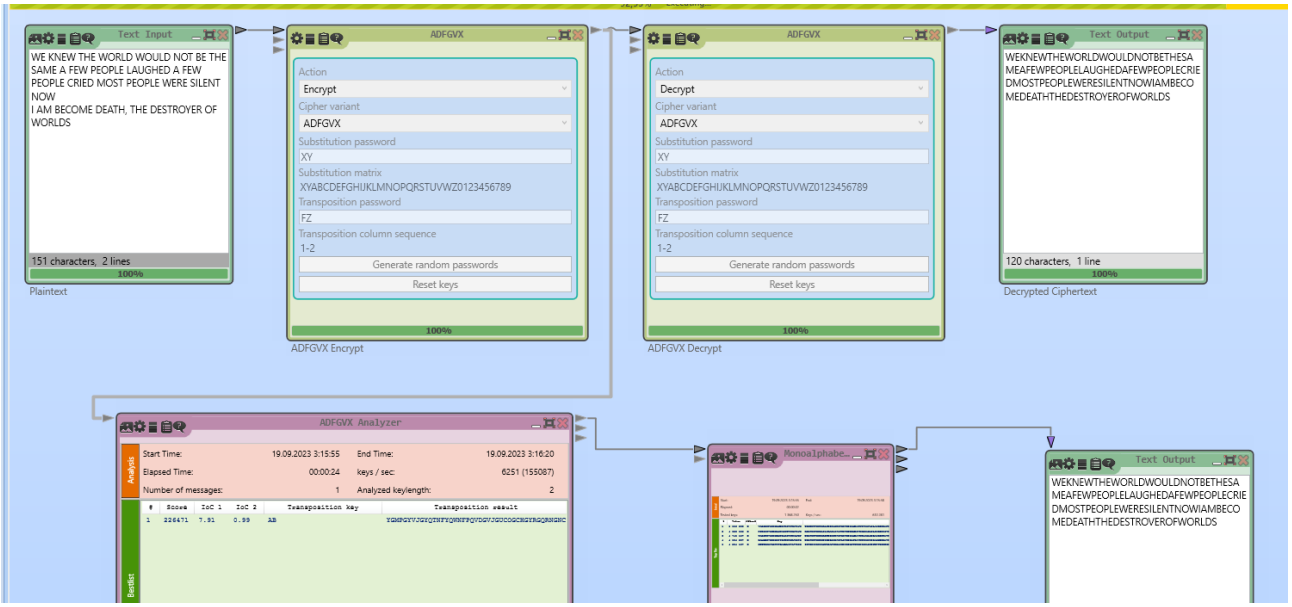

Рисунок 12: атака на ADFGVX

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.