Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Лабораторная работа № 1-3

Изучение классических шифров

Студент: _____ Чернякова Валерия, группа 1304

Руководитель: _____ Племянников А.К., доцент каф. ИБ

Санкт-Петербург 2024

Цель работы

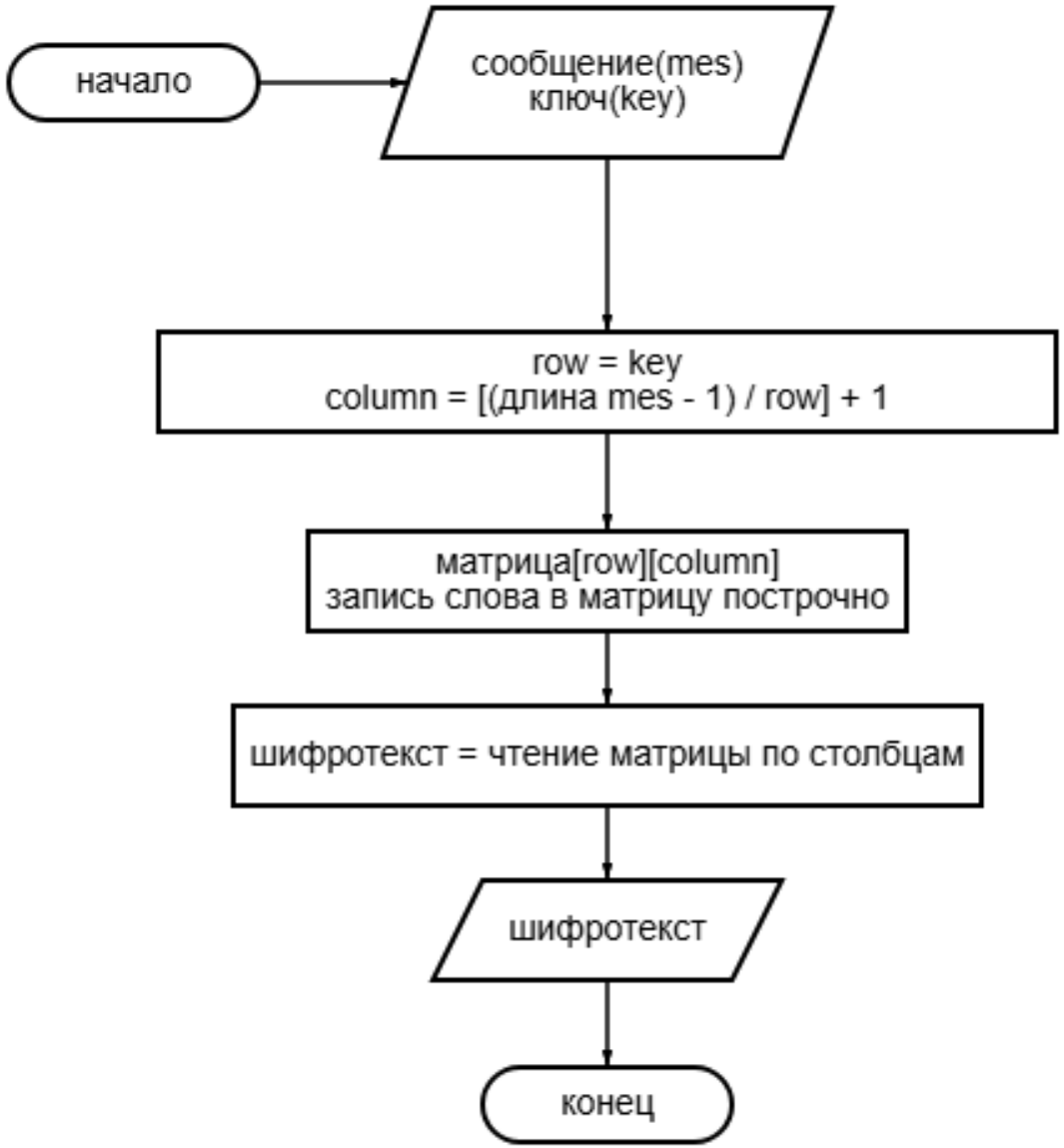
Исследовать шифры Scytale, Caesar, Substitution, Permutation/Transposition, Vigenere, Hill, ADFGVX и получить практические навыки работы с ними, в том числе с использованием приложений CrypTool 1 и 2.

Шифр «Сцитала» (Scytale)

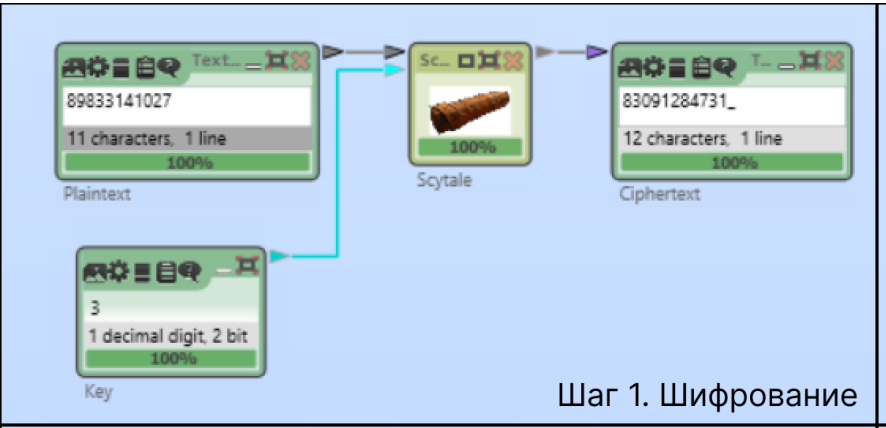
Задание

1. Найти шифр в CrypTool.
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. Выполнить самостоятельную работу: взять в CrypTool 2 шаблон атаки на шифр методом «грубой силы» и модифицировать этот шаблон, заменив блок с шифротекстом на блок ввода открытого текста и блок зашифрования. Изучить принципы этой автоматической атаки.

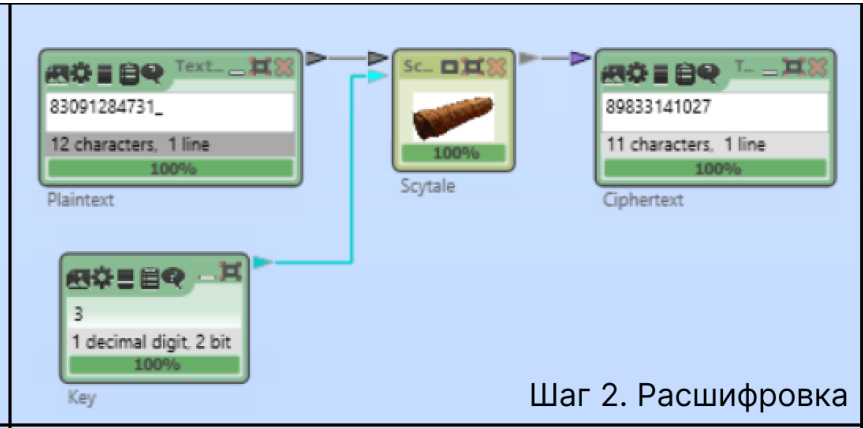
Схема работы шифра



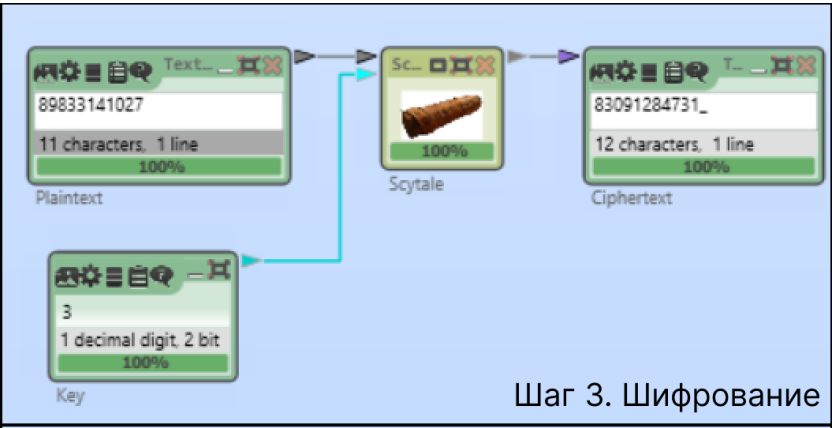
Шифрование и расшифровка последовательности цифр



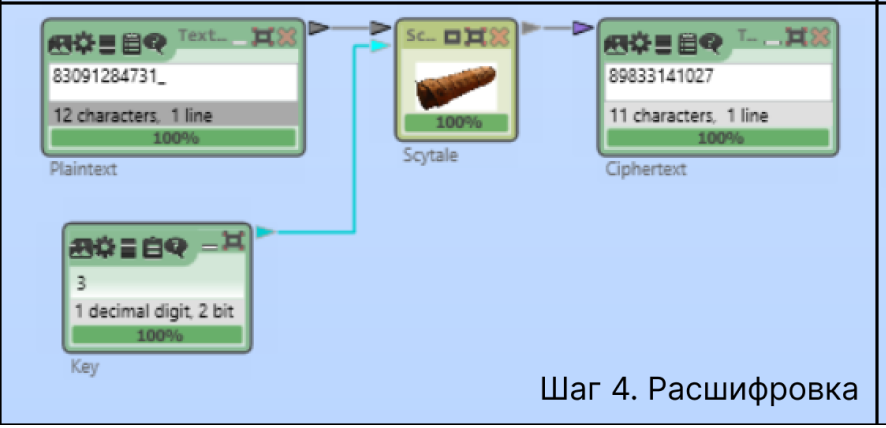
Шаг 1. Шифрование



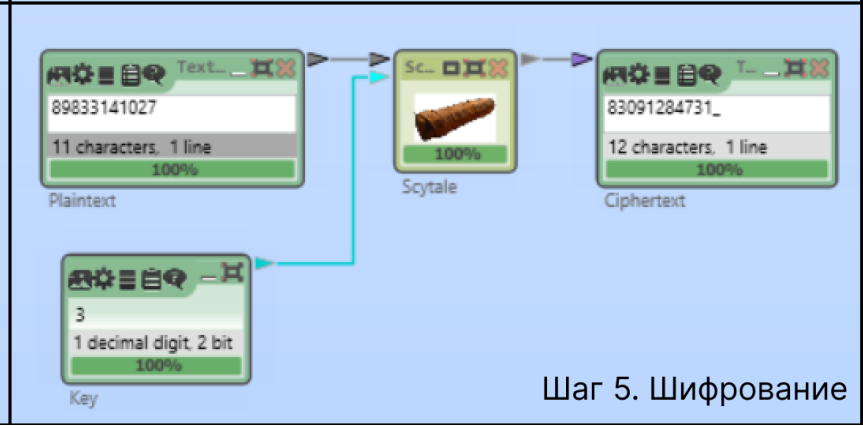
Шаг 2. Расшифровка



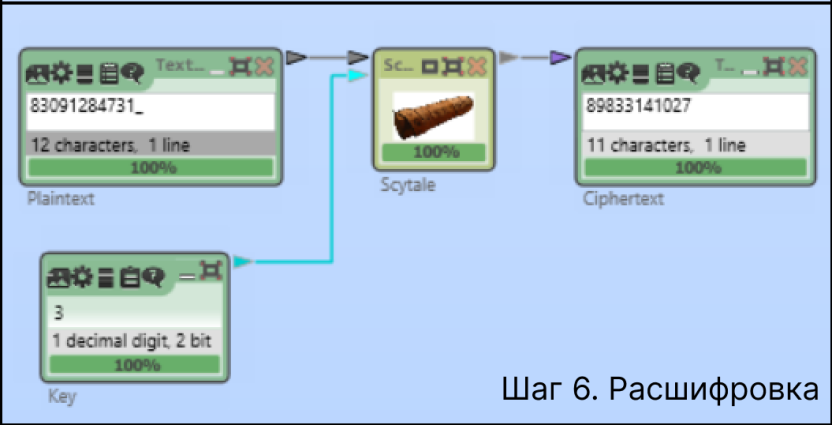
Шаг 3. Шифрование



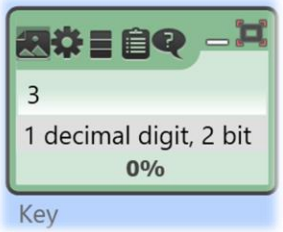
Шаг 4. Расшифровка



Шаг 5. Шифрование



Шаг 6. Расшифровка



Значение, указываемое в данном окне (key), соответствует *Number of Edges* (количество граней цилиндра)

Шифрование и расшифровка фамилии

Вручную

Number of Edges = 4

CHE|RNY|AKO|VA_

C H E
R N Y
A K O
V A _

CRAVHNKAEYO_

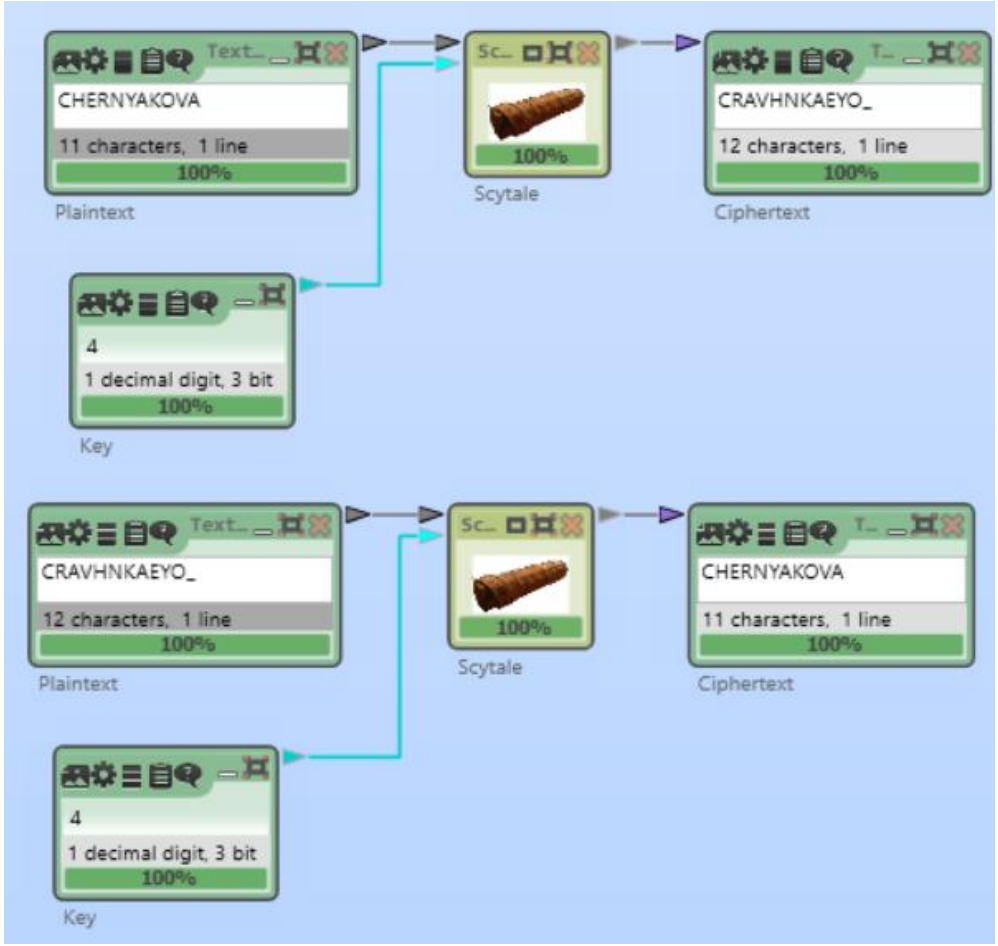
CRAV|HNKA|EYO_

C H E
R N Y
A K O
V A _

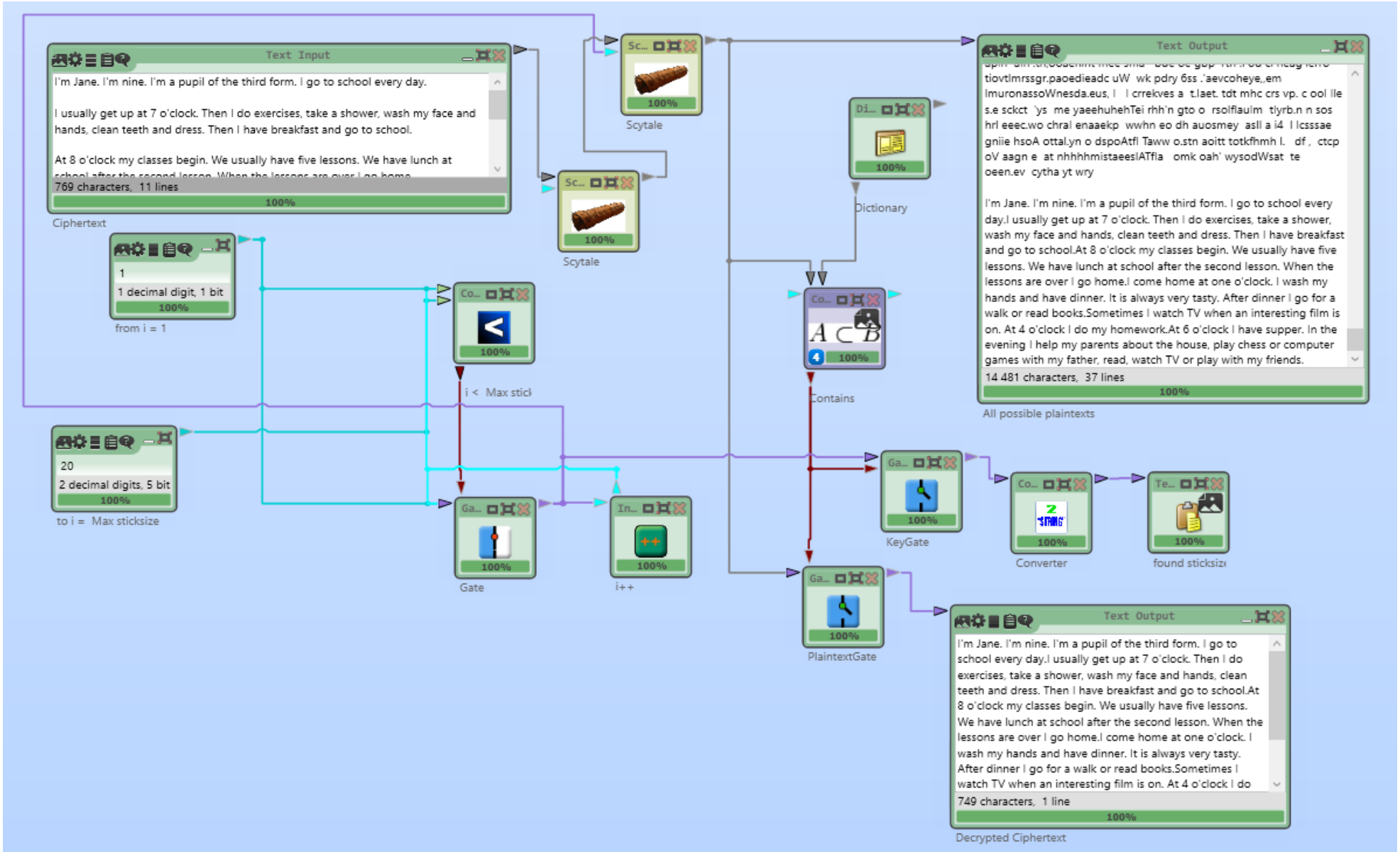
CHERNYAKOVA

С применением CrypTool2

Number of Edges = 4



Атака на шифр методом «грубой силы»



Заключение

- Изучен шифр «Сцитала» и выявлены его следующие основные характеристики:

  Тип шифра – перестановка;

  Ключ шифра – количество граней цилиндра.

- Проведена атака методом грубой силы на шифр «Сцитала» и выявлены ее следующие основные характеристики:

  Оценка сложности атаки следующая:

  O(n), где n – длина зашифрованного текста.

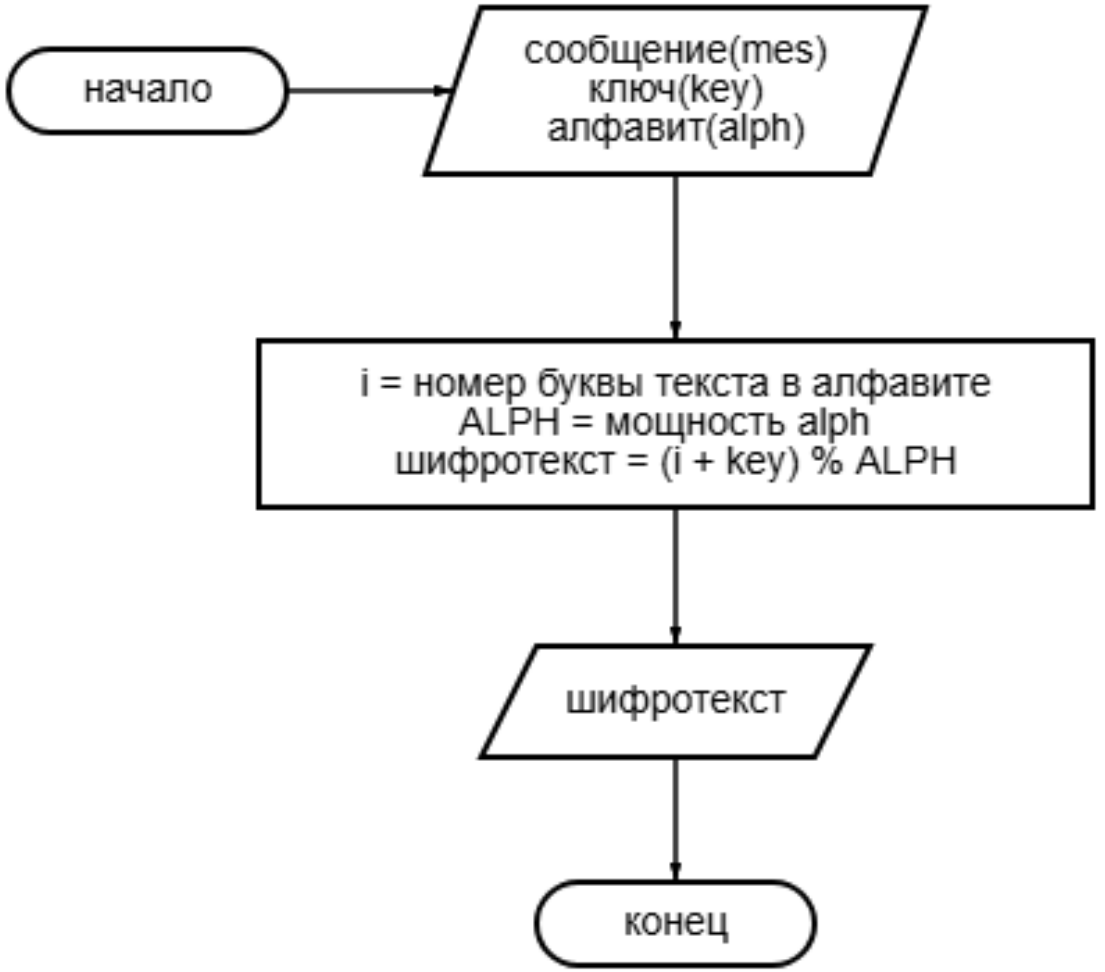
  O(n^2), когда используется смещение.

Шифр Цезаря (Caesar)

Задание

1. Найти шифр в CrypTool.
2. Зашифровать и расшифровать текст, содержащий только фамилию (транслитерация латиницей), вручную и с помощью шифра с ключом, отличным от 0. Убедиться в совпадении результатов.
3. Построить гистограмму частот букв английского языка по эталонному файлу English.txt (папка CrypTool/reference).
4. Зашифровать ключом отличным от 0 файл CrypTool-en.txt (папка CrypTool/Examples).
5. Построить гистограмму частот букв в зашифрованном тексте, сравнить визуально гистограммы и подтвердить ключ зашифрования.
6. Проверить гипотезу о значении ключа утилитой Analysis –> Symmetric Encryption(Classic) –> Cipher Text Only –> Caesar.

Схема работы шифра



Шифрование и расшифровка фамилии

Вручную

Key = 10

CHERNYAKOVA

▼

ABCDEFGHIJKLMNOPQRSTUVWXYZ

KLMNOPQRSTUVWXYZABCDEFGHIJ

▼

MROBXIKUYFK

MROBXIKUYFK

▼

ABCDEFGHIJKLMNOPQRSTUVWXYZ

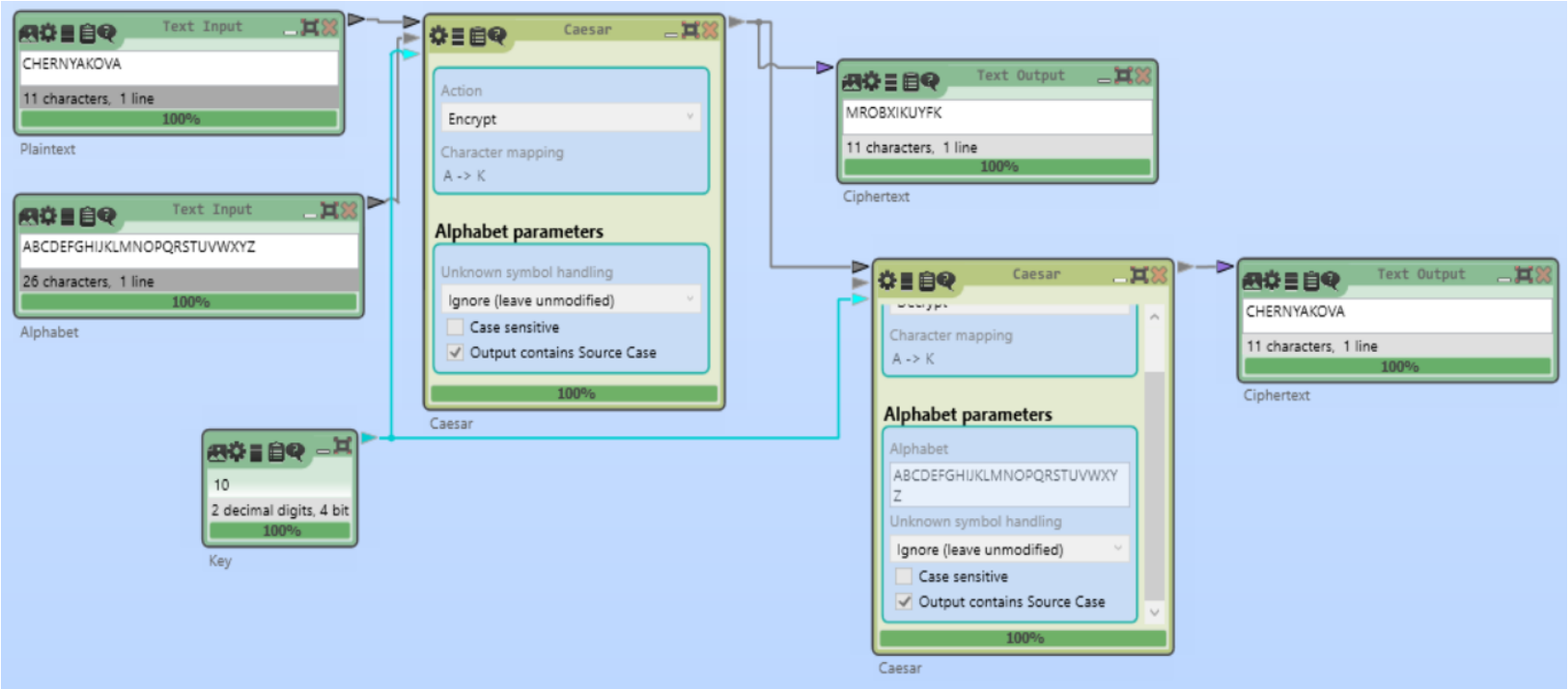
KLMNOPQRSTUVWXYZABCDEFGHIJ

▼

CHERNYAKOVA

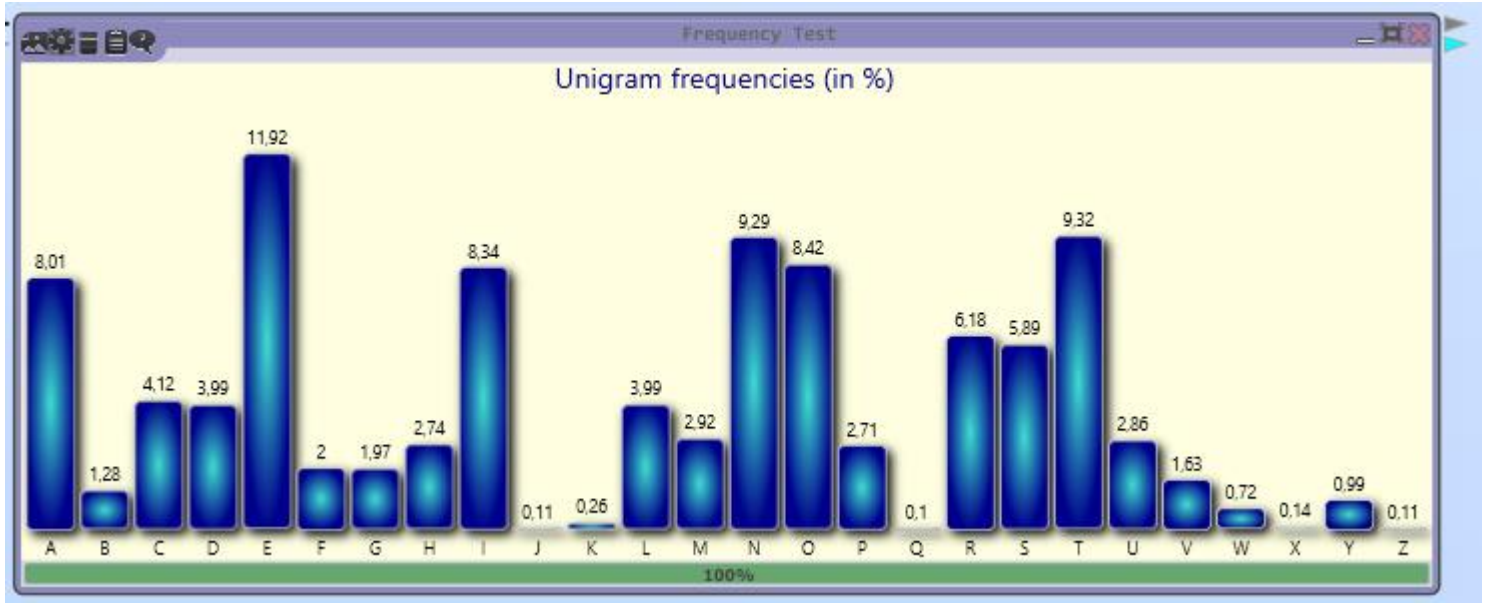
С применением CrypTool2

Key = 10

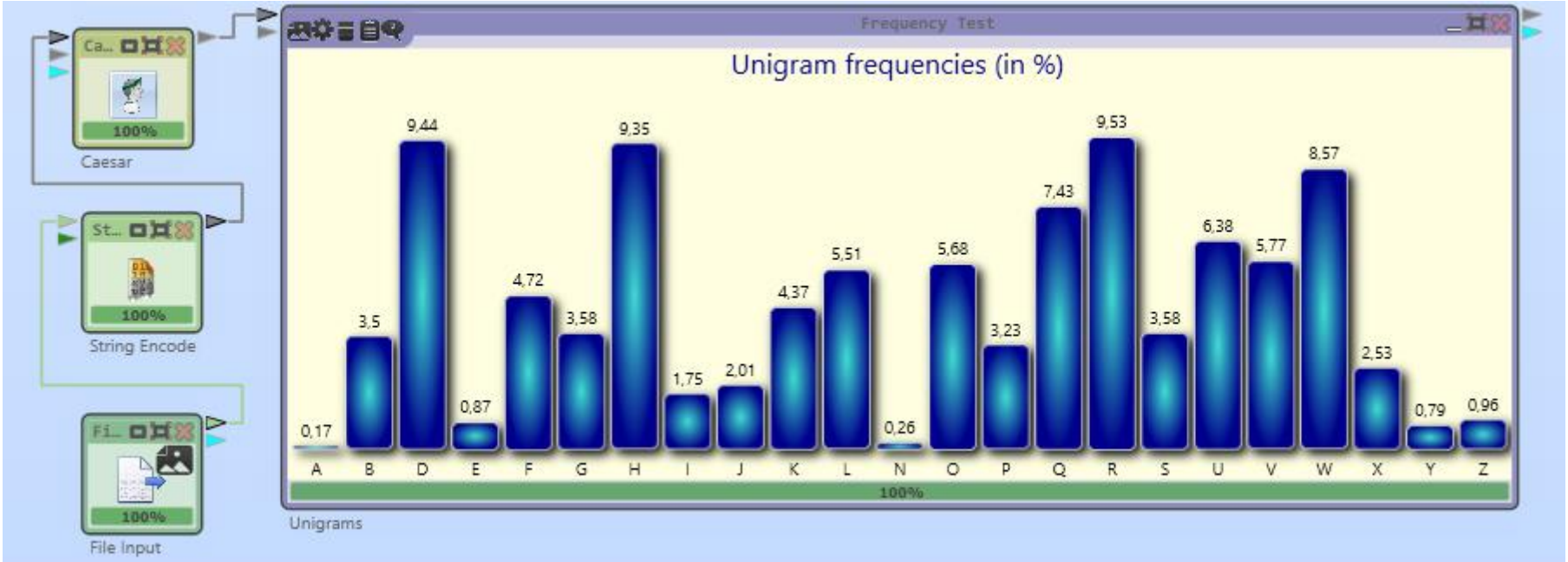


Сравнения гистограмм частот символом

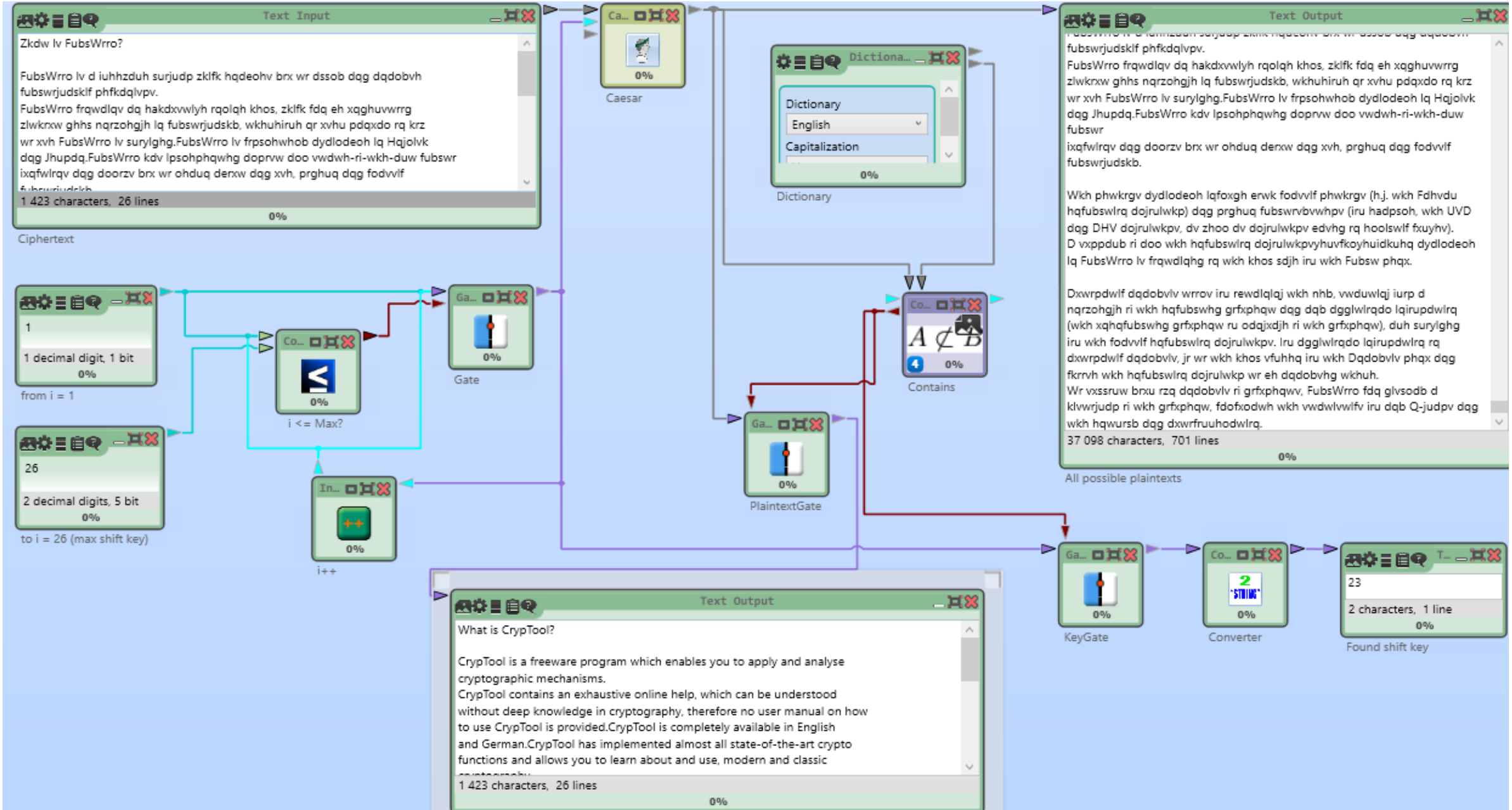
Файл *CrypTool-en.txt* был зашифрован с ключом *key = 3*. То есть *A -> D*. Гистограмма представлена снизу.
Справа представлена гистограмма текста *English.txt*.



Если начать сравнивать гистограммы, то можно заметить, что при соблюдении смещения и расположении графиков друг под другом, они совпадают.



Атака с помощью анализа частот символов



Заключение

- Изучен шифр Цезаря и выявлены его следующие основные характеристики:

  Тип шифра – замена;

  Ключ шифра – смещение по алфавиту.

- Проведена атака методом грубой силы на шифр Цезаря и выявлены ее следующие основные характеристики:

  Оценка сложности атаки следующая:

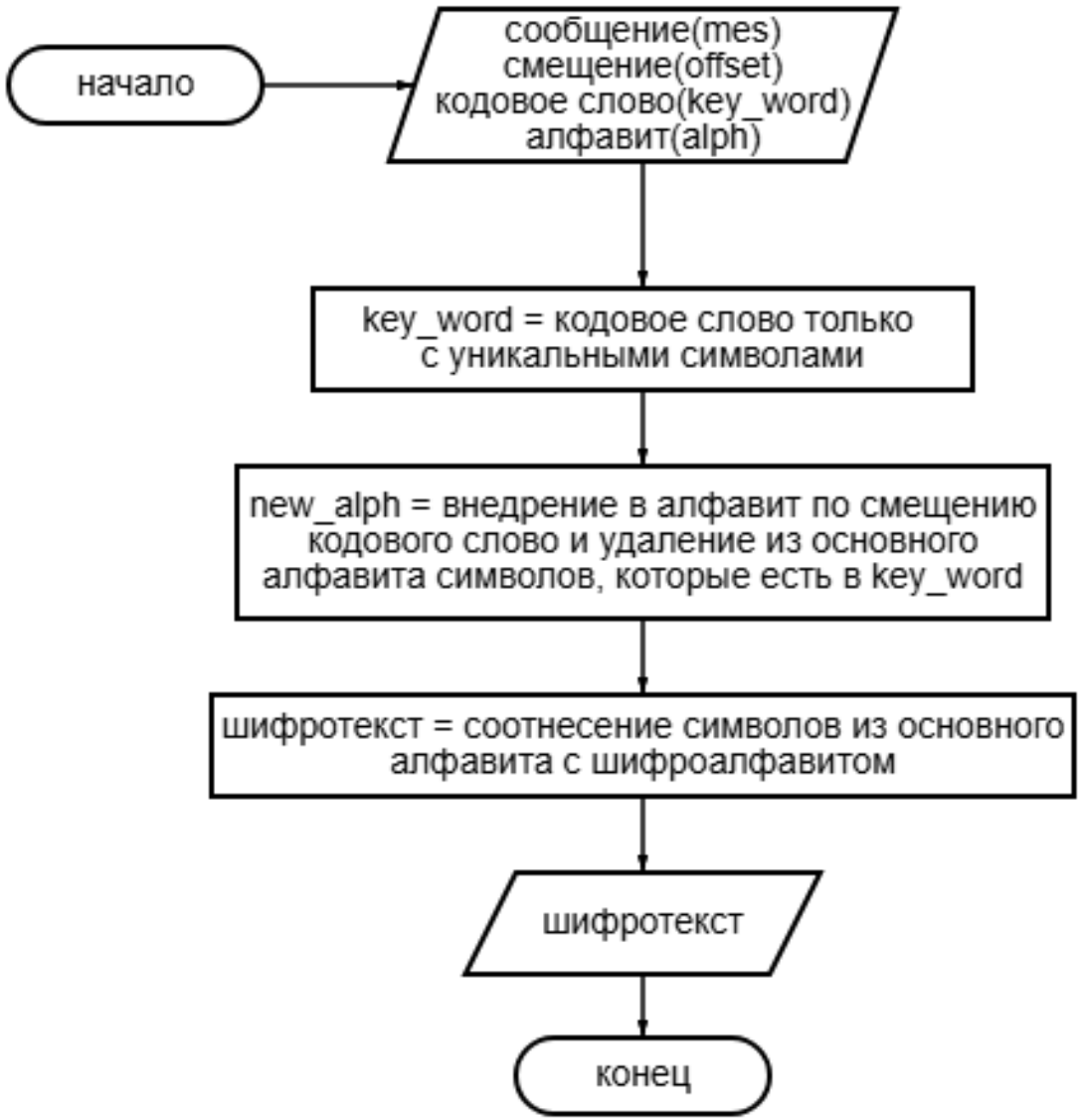
  $O(n)$, где n – мощность алфавита.

Шифр моноалфавитной подстановки (Substitution)

Задание

1. Найти шифр в CrypTool .
2. Зашифровать и расшифровать текст, содержащий только вашу фамилию (транслитерация латиницей), вручную и с помощью шифра с выбранным ключом и смещением Offset ≠ 0. Убедиться в совпадении результатов.
3. Выполнить зашифрование и расшифрование с различными паролями и смещениями Offset и разобраться, как формируется алфавит шифротекста.
4. Выбрать абзац (примерно 600 символов) из файла English.txt (папка CrypTool/reference) и зашифровать его.
5. Выполнить атаку на шифротекст, используя приложение из Analysis –> Symmetric Encryption(classic) –> Cipher Text Only.
6. Повторить шифрование и атаку для тестов примерно в 300 и 150 символов.
7. Изучить возможности CrypTool 1 для автоматизации выполнения ручного расшифрования для текстов размером менее 300 символов.
8. Выбрать новый абзац (примерно 600 символов) из файла English.txt (папка CrypTool/reference) и зашифровать его.
9. Дешифровать этот абзац, используя приложение Analysis –> Tools for Analysis и Analysis –> Symmetric Encryption(classic) –> Manual Analysis.

Схема работы шифра



Шифрование и расшифровка фамилии

Вручную

Key = SCHOOL, Offset = 7

CHERNYAKOVA

▼

ABCDEFGHIJKLMNOPQRSTUVWXYZ

TUVWXYZSCHOLABDEFGIJKMNPQR

▼

VSXGBQTODMT

VSXGBQTODMT

▼

TUVWXYZSCHOLABDEFGIJKMNPQR

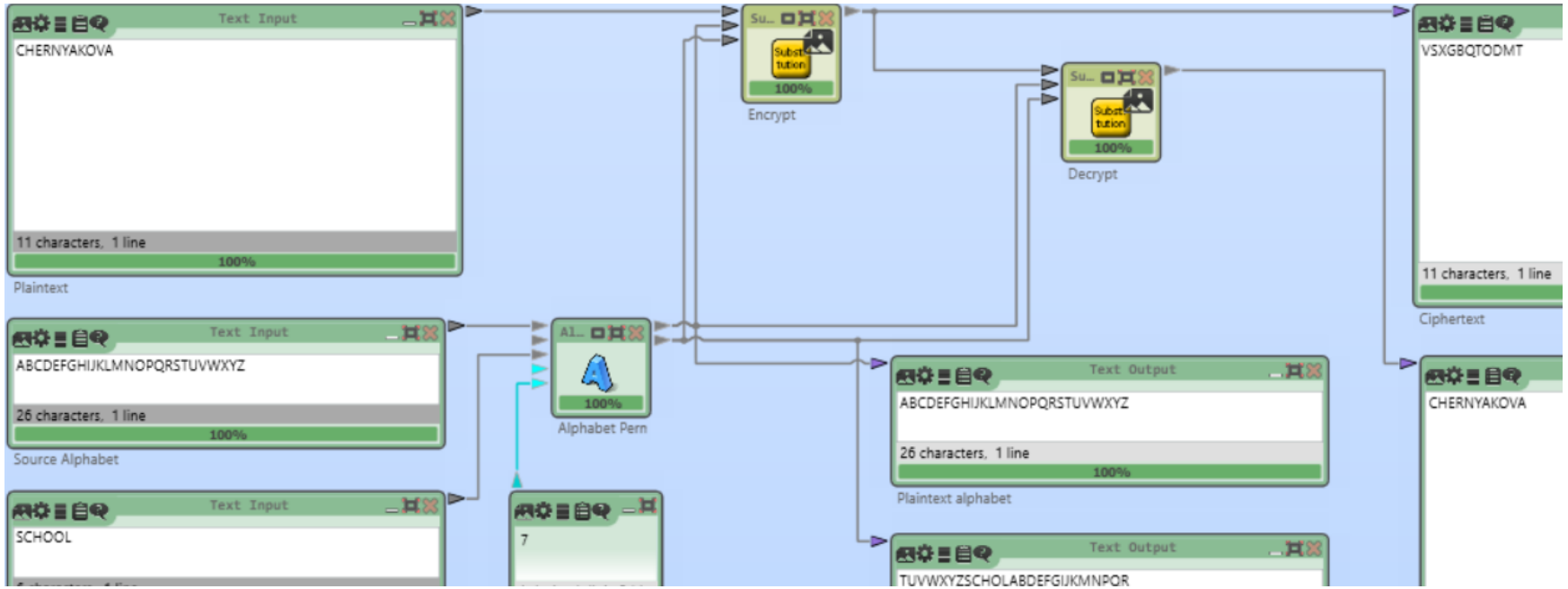
ABCDEFGHIJKLMNOPQRSTUVWXYZ

▼

CHERNYAKOVA

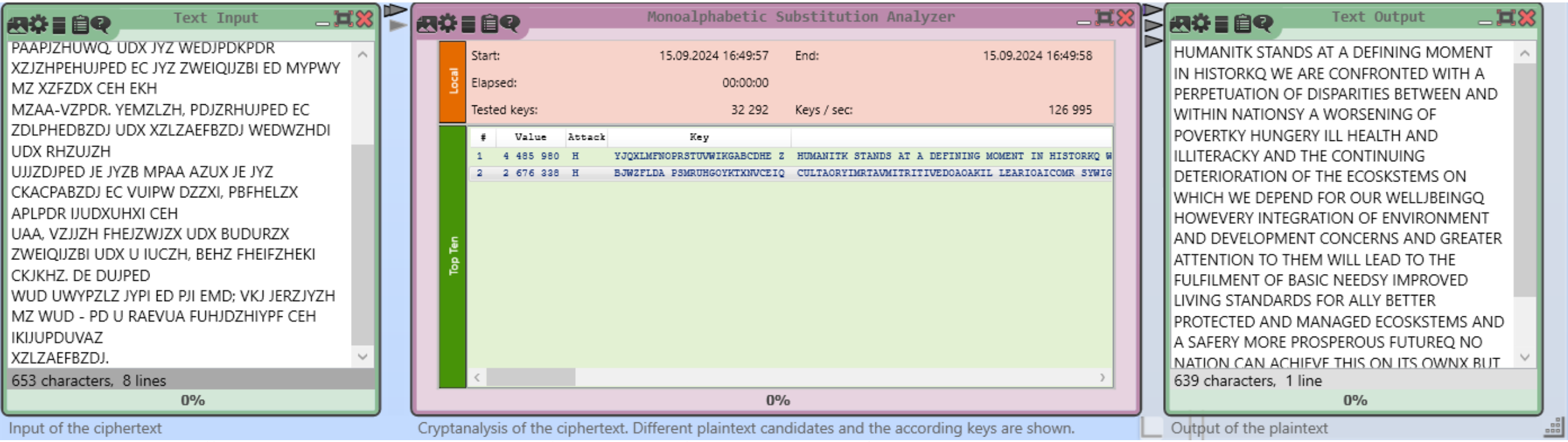
С применением CrypTool2

Key = SCHOOL, Offset = 7

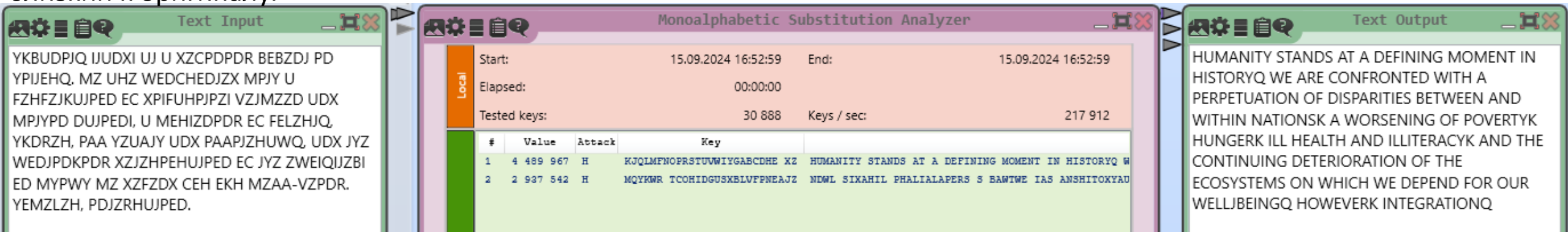


Атака на шифр

Зашифрованный текст из 600 символов (примерно). Ключ подобран неверно, но при расшифровке получился текст близкий к оригиналу.

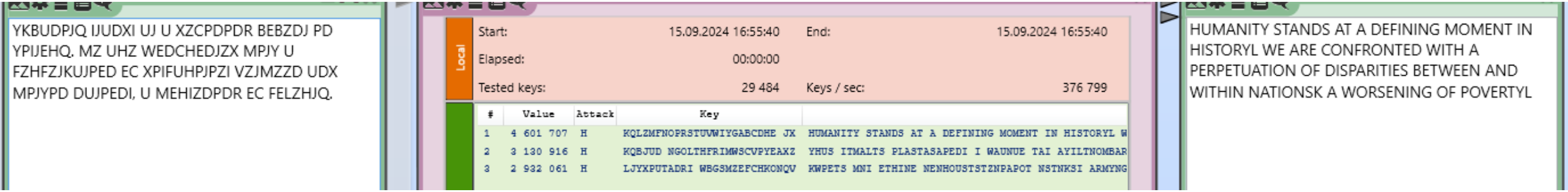


Зашифрованный текст из 300 символов (примерно). Ключ подобран неверно, но при расшифровке получился текст близкий к оригиналу.

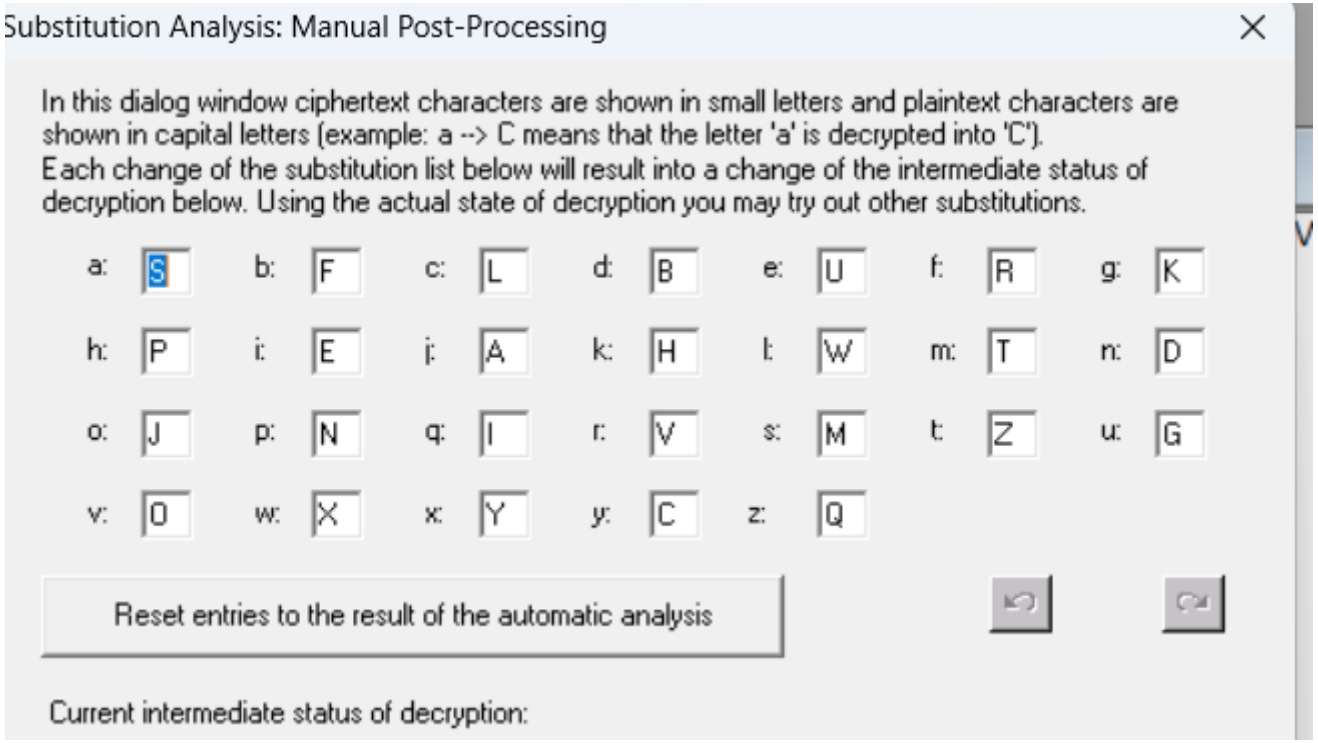


Атака на шифр

Зашифрованный текст из 150 символов (примерно). Ключ подобран неверно, но при расшифровке получился текст близкий к оригиналу.



В CrypTool 1 предусмотрена возможность для ручного улучшения дешифрования текстов, объем которых составляет меньше 300 символов.



Заключение

- Изучен шифр моноалфавитной подстановки и выявлены его следующие основные характеристики:

  Тип шифра – замена;

  Ключ шифра – кодовое слово + смещение.

- Проведена атака методом грубой силы на шифр моноалфавитной подстановки и выявлены ее следующие основные характеристики:

  Оценка сложности атаки следующая:

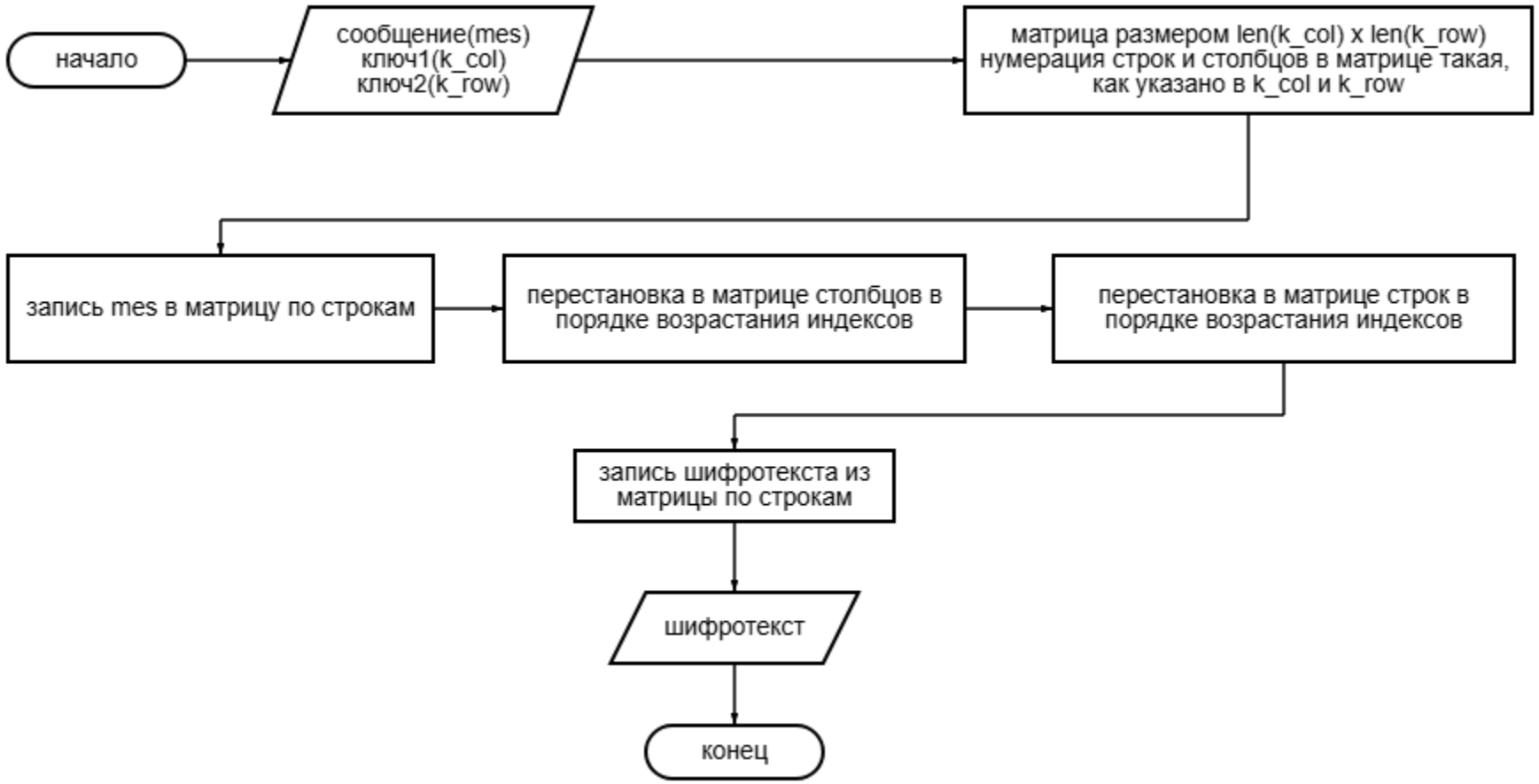
  $O(n!)$, где n – мощность алфавита.

Шифр двойной перестановки (Permutation/Transposition)

Задание

1. Найти шифр в CrypTool 2.
2. Зашифровать и расшифровать текст, содержащий ваши ФамилиюИмяОтчество (транслитерация латиницей), вручную и с помощью шифра с ключами для перестановки столбцов и строк. Убедиться в совпадении результатов.
3. Выполнить зашифрование и расшифрование с различными ключами и с различными вариантами перестановки матрицы с текстом по строкам и столбцам. Разобраться с параметрами утилиты.
4. Зашифровать текст, содержащий ФамилиюИмяОтчество, и провести атаку, основанную на знании исходного текста, Analysis –> Symmetric Encryption(classic) –> Known Plaintex.

Схема работы шифра



Шифрование и расшифровка ФИО

Столбцы = 3, 2, 1, 4 Строки = 1, 2, 8, 7, 4, 5, 3, 6

Вручную

ChernyakovaValeriyaAlekseevna

	3	2	1	4
1	C	h	e	r
2	n	y	a	k
8	o	v	a	V
7	a	l	e	r
4	i	y	a	A
5	l	e	k	s
3	e	e	v	n
6	a			

	1	2	3	4
1	e	h	C	r
2	a	y	n	k
8	a	v	o	V
7	e	l	a	r
4	a	y	i	A
5	k	e	l	s
3	v	e	e	n
6			a	

	1	2	3	4
1	e	h	C	r
2	a	y	n	k
3	v	e	e	n
4	a	y	i	A
5	k	e	l	s
6			a	
7	e	l	a	r
8	a	v	o	V

ehCraynkveenayiAkels__a_elaravoV

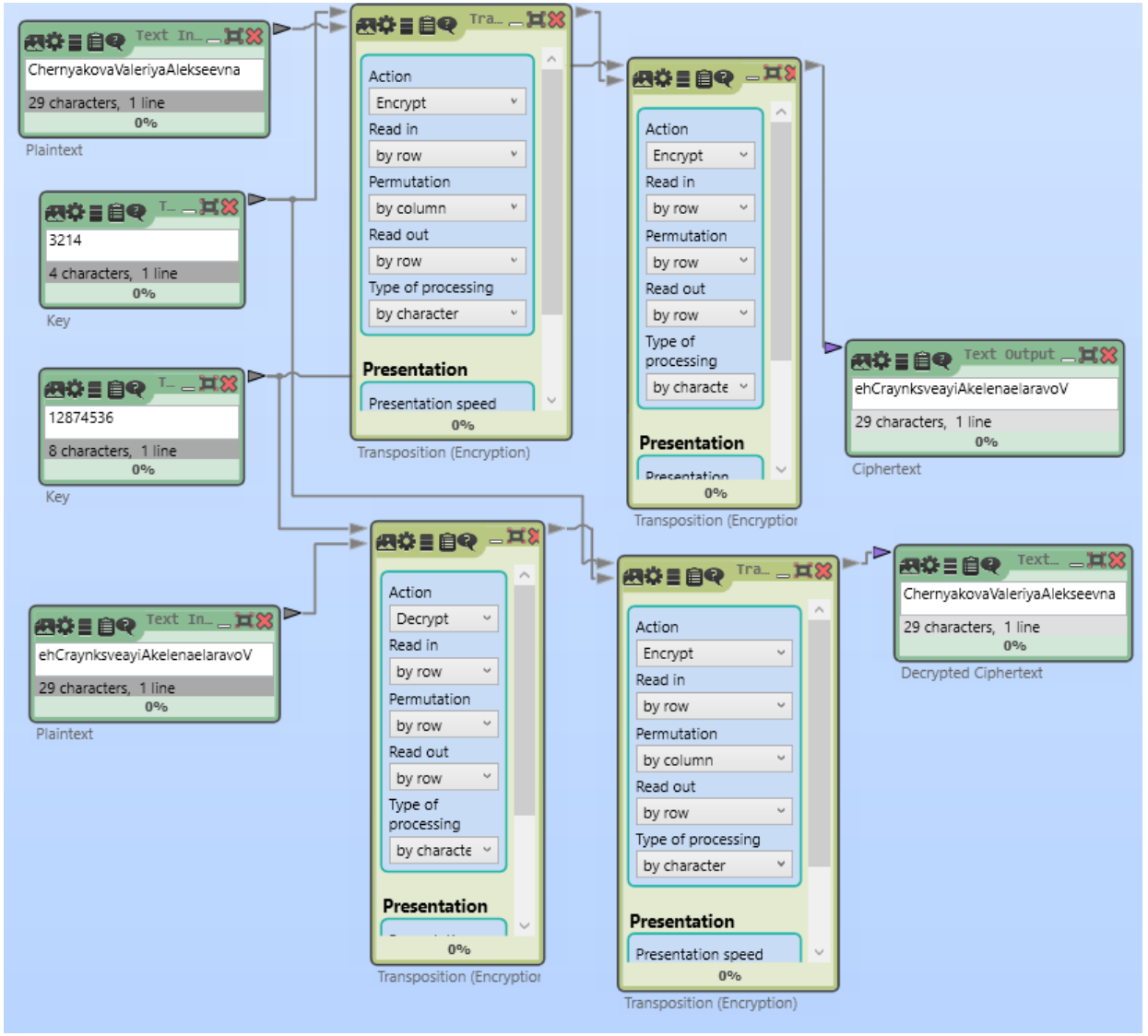
	1	2	3	4
1	e	h	C	r
2	a	y	n	k
3	v	e	e	n
4	a	y	i	A
5	k	e	l	s
6			a	
7	e	l	a	r
8	a	v	o	V

	1	2	3	4
1	e	h	C	r
2	a	y	n	k
8	a	v	o	V
7	e	l	a	r
4	a	y	i	A
5	k	e	l	s
3	v	e	e	n
6			a	

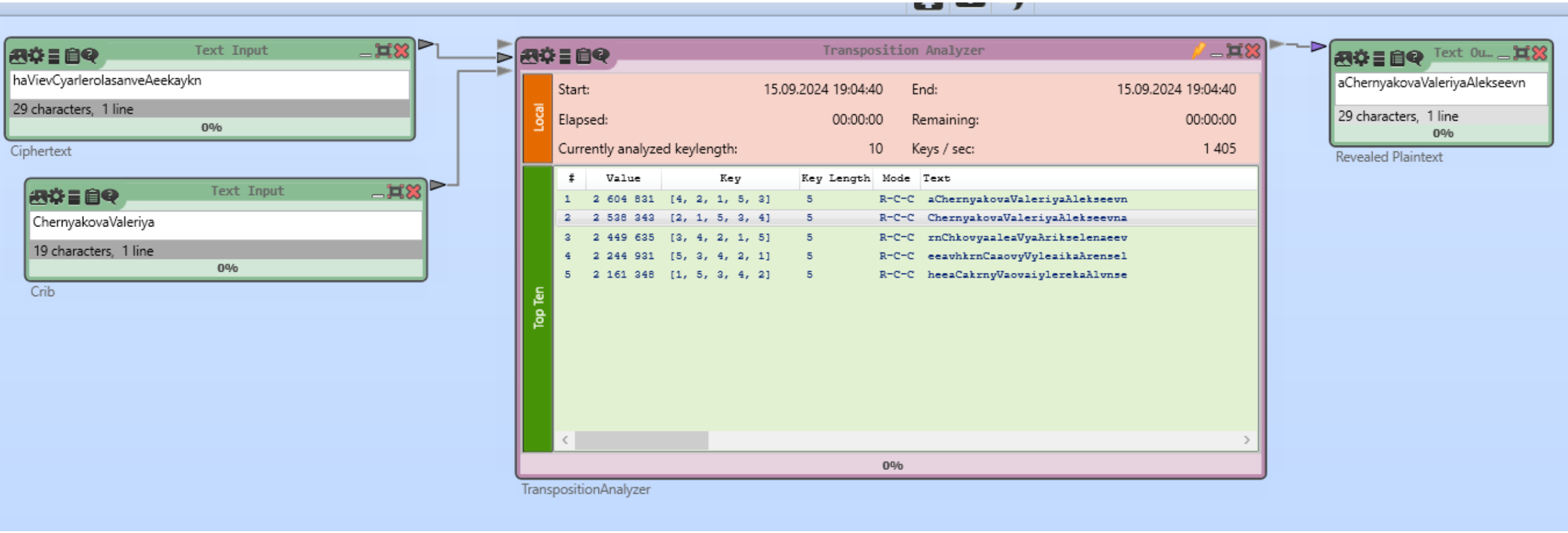
	3	2	1	4
1	C	h	e	r
2	n	y	a	k
8	o	v	a	V
7	a	l	e	r
4	i	y	a	A
5	l	e	k	s
3	e	e	v	n
6	a			

ChernyakovaValeriyaAlekseevna

С применением CrypTool2



Атака на шифр, основанная на знании исходного текста



Заключение

- Изучен шифр двойной перестановки и выявлены его следующие основные характеристики:

  Тип шифра – перестановка;

  Ключ шифра – значения перестановок строк и столбцов.

- Проведена атака методом грубой силы на шифр двойной перестановки и выявлены ее следующие основные характеристики:

  Оценка сложности атаки следующая:

  $O(n! * m!)$, где n и m – количество строк и столбцов матрицы.

Шифр Виженера (Vigenere)

Задание

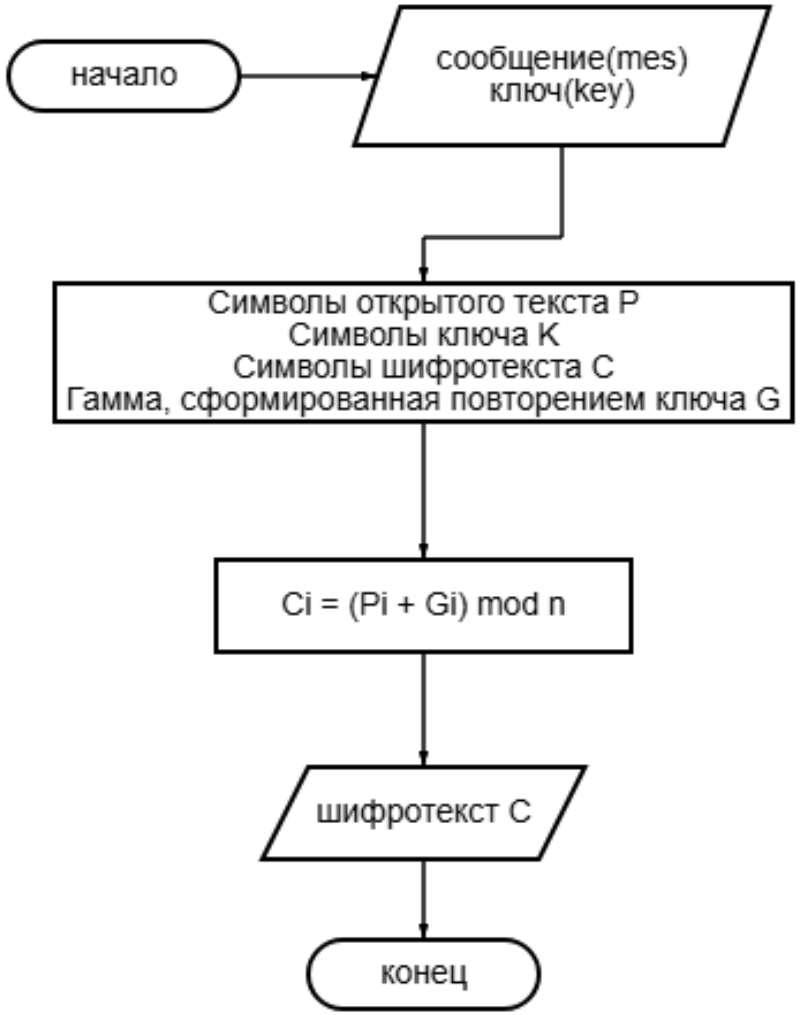
1. Найти шифр в CrypTool 2.
2. Зашифровать и расшифровать текст, содержащий только вашу фамилию (транслитерация латиницей), вручную и с помощью шифра с выбранным ключом. Убедиться в совпадении результатов.
3. Провести атаку на шифротекст, используя приложение Analysis –> Symmetric Encryption(Classic) –> Cipher Text Only –> Vigenere.
4. Повторить атаку для фрагмента текста из файла English.txt (папка CrypTool/reference). Размер текста – не менее 1000 символов.
5. Воспроизвести эту атаку в автоматизированном режиме:

а) определить размер ключа с помощью приложения Analysis –> Tools for Analysis –> Autocorrelation;

б) выполнить перестановку текста с размером столбца, равным размеру ключа, приложением Permutation/Transposition;

в) определить очередную букву ключа приложением Analysis –> Symmetric Encryption(Classic) –> Cipher Text Only –> Caesar.

Схема работы шифра



Количество элементов, входящих
в G равно [mes/key] + 1
n - мощность алфавита

Шифрование и расшифровка ФИО

Кодовое слово = PHONE

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

C	H	E	R	N		Y	A	K	O	V		A				
P	H	O	N	E		P	H	O	N	E		P	H	O	N	E
R	O	S	E	R		N	H	Y	B	Z		P				

▼

ROSERNHYBZP

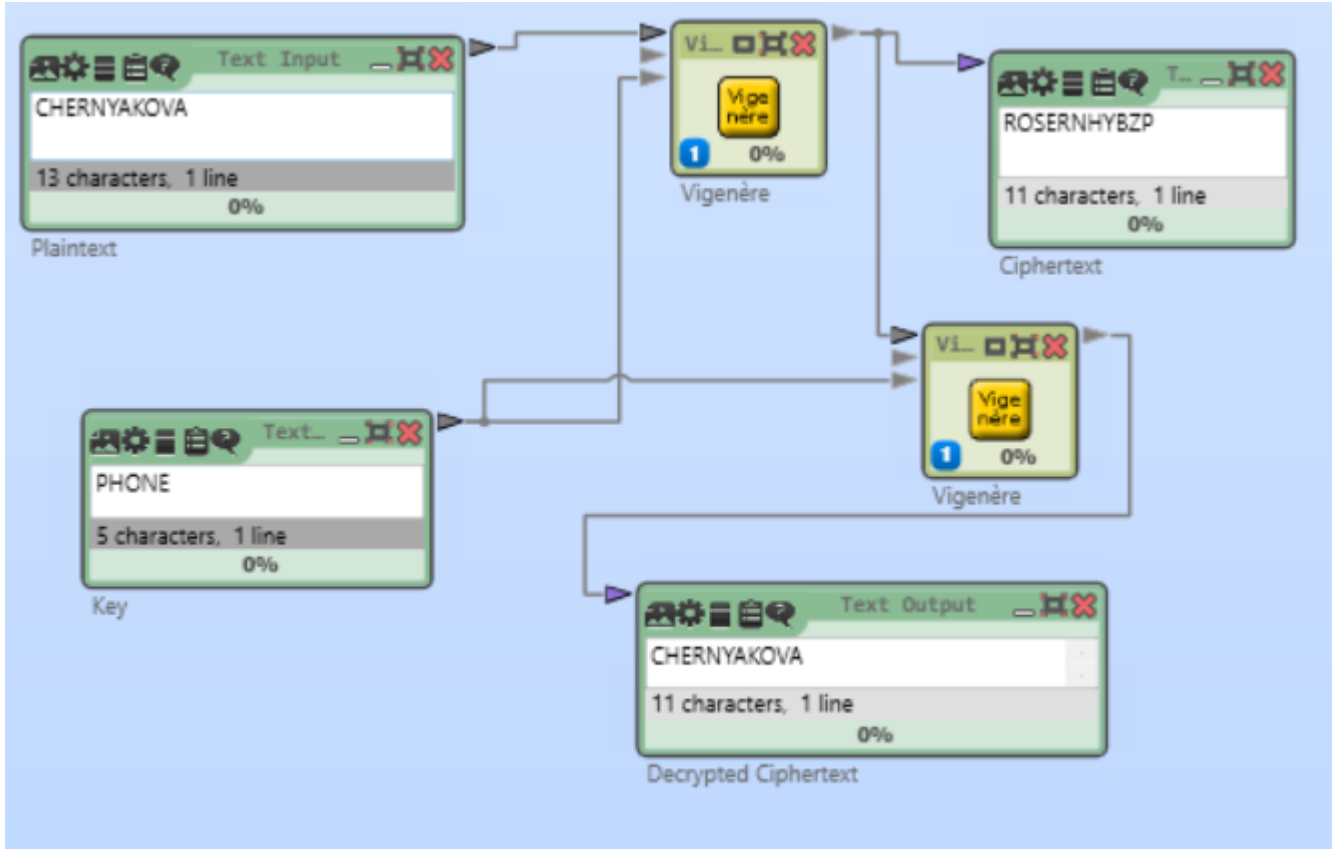
▼

R	O	S	E	R		N	H	Y	B	Z		P				
P	H	O	N	E		P	H	O	N	E		P	H	O	N	E
C	H	E	R	N		Y	A	K	O	V		A				

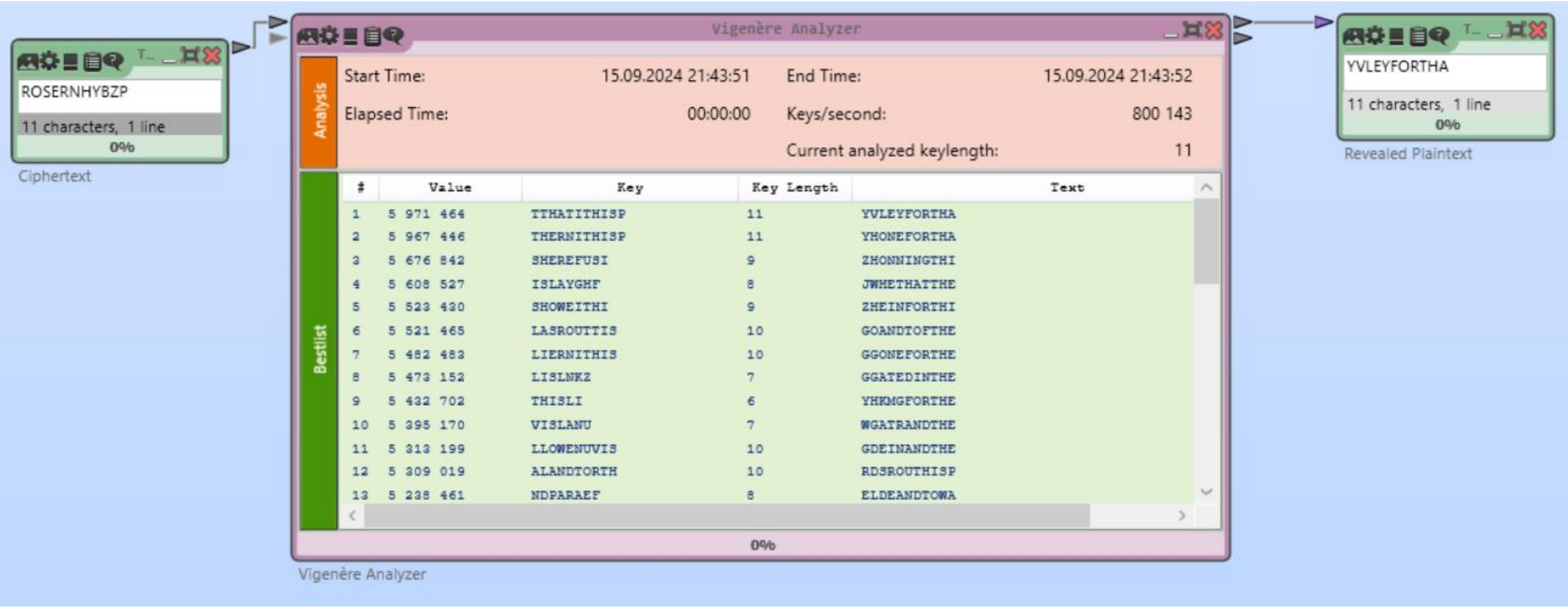
▼

CHERNYAKOVA

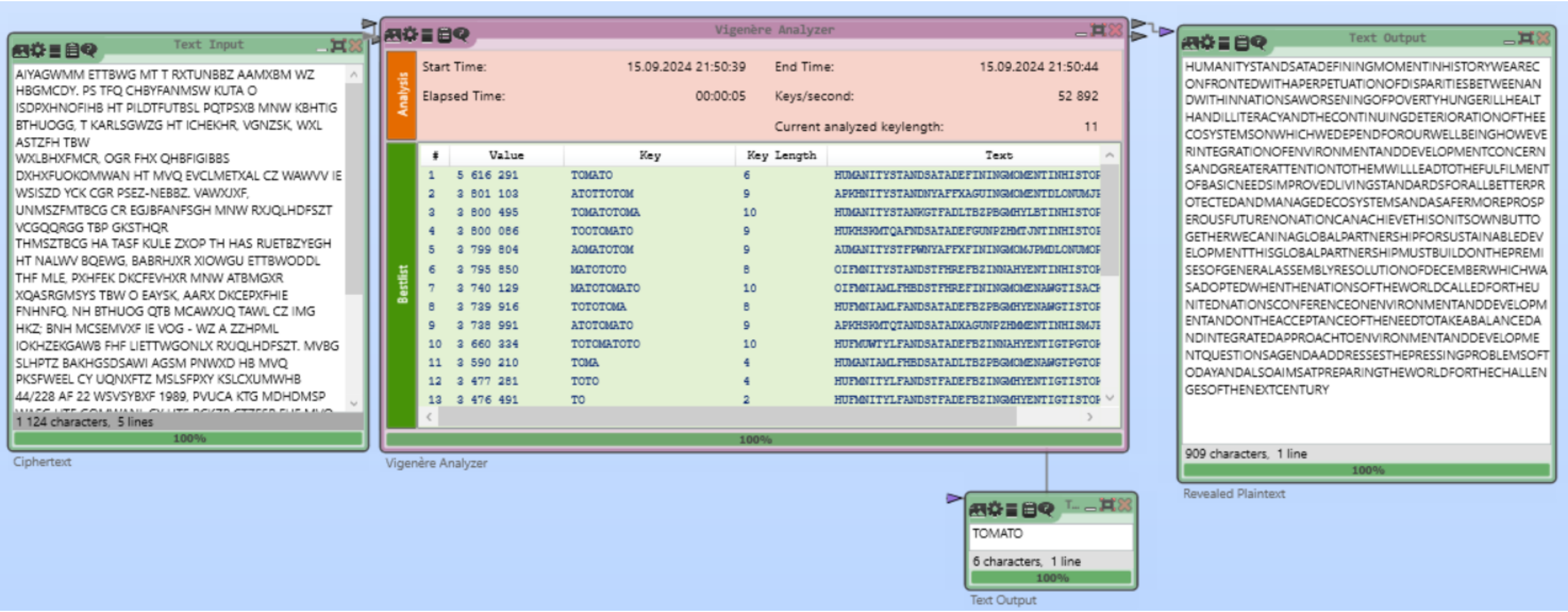
С применением CrypTool2



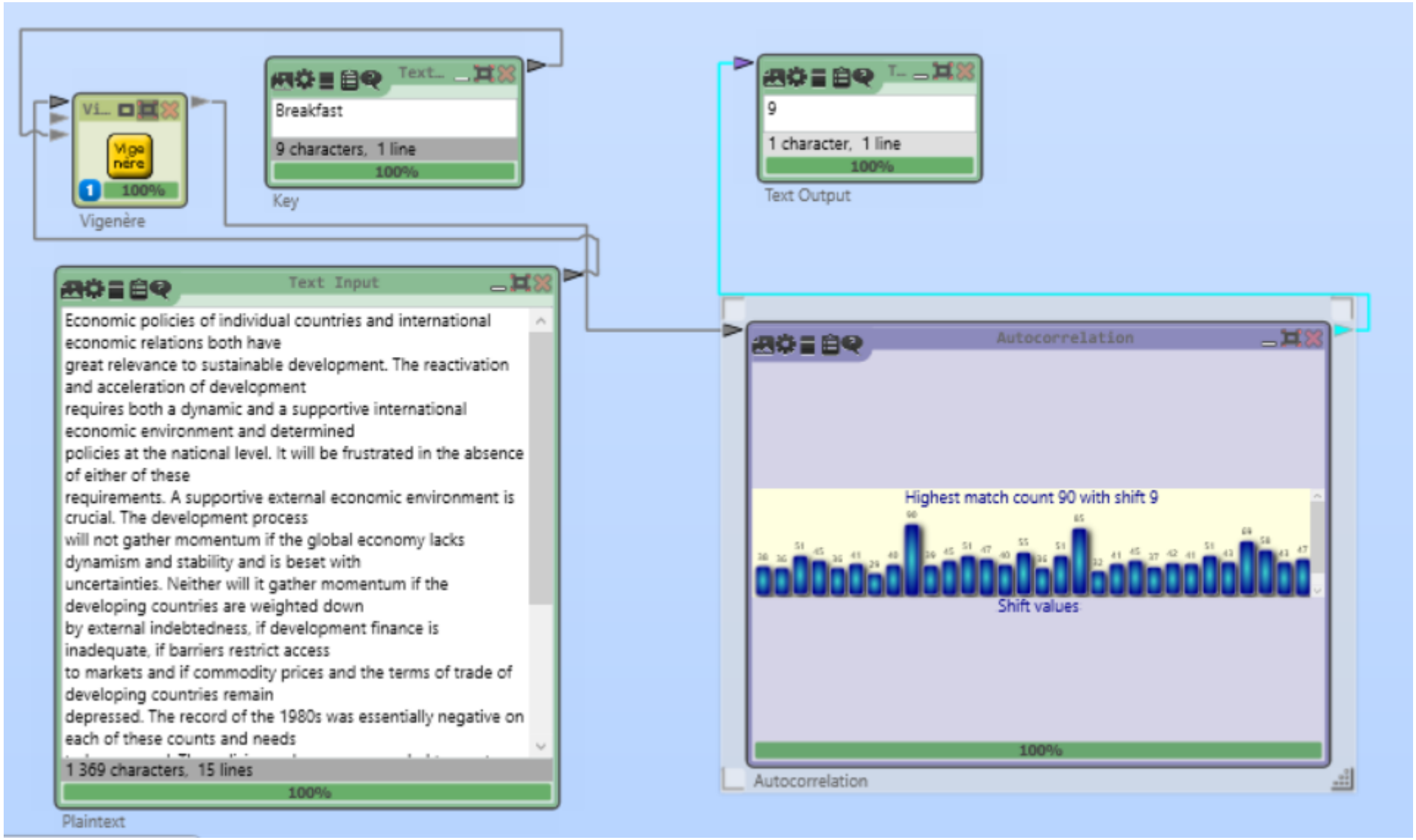
Атака на шифр



Атака на шифр (текст из файла English.txt)

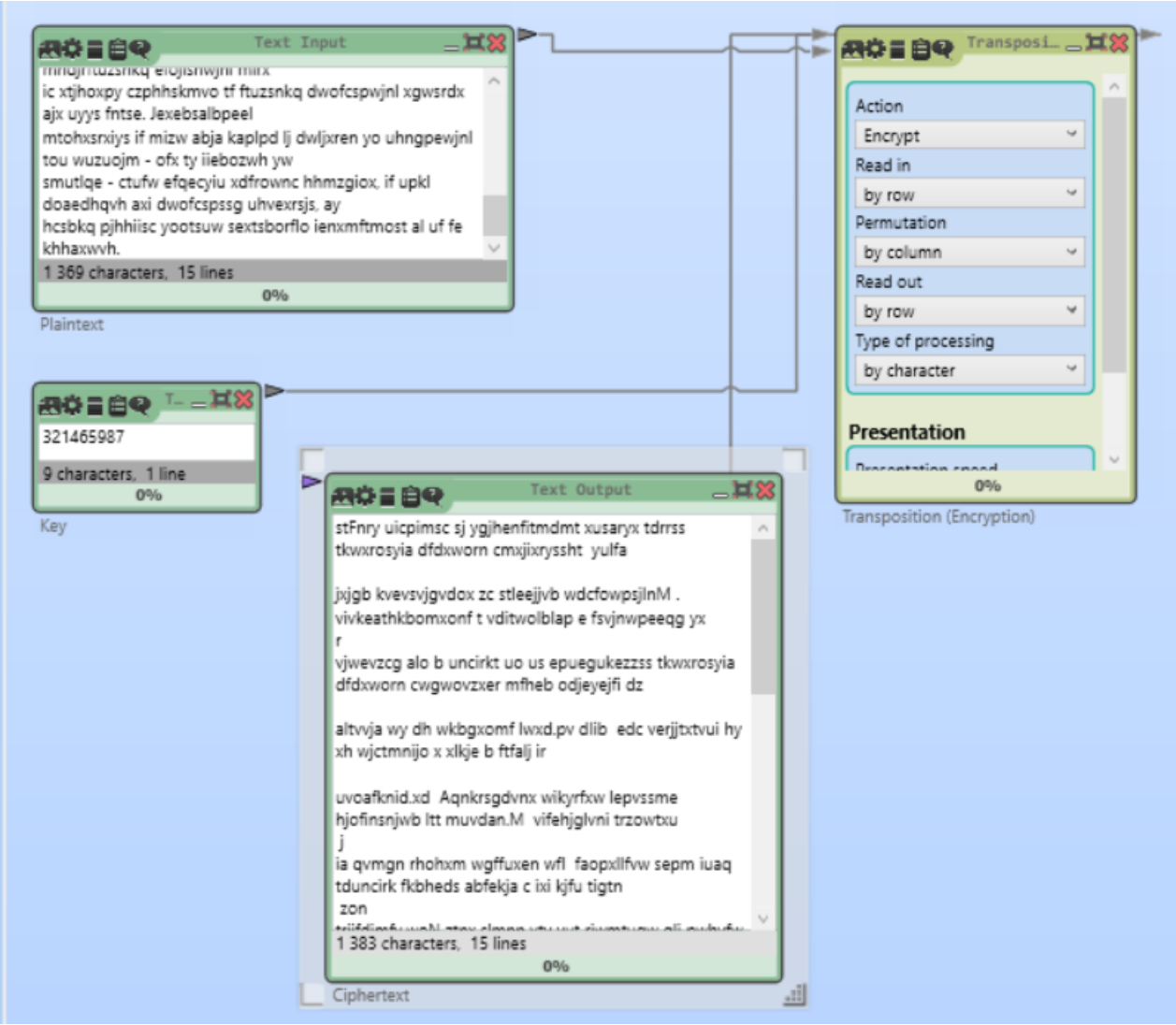


Атака на шифр в автоматизированном режиме



Определение размера ключа с помощью autocorrelation

Атака на шифр в автоматизированном режиме



Перестановка текста с размером столбца, равным размеру ключа.
Далее необходимо будет сгруппировать части текста, зашифрованные одной буквой.
На каждую часть будет проведена атака аналогичная на шифр Цезаря.
Так будет получена отдельно каждая буква ключа.

Заключение

- Изучен шифр Виженера и выявлены его следующие основные характеристики:

  Тип шифра – замена;

  Ключ шифра – кодовое слово.

- Проведена атака методом грубой силы на шифр Виженера и выявлены ее следующие основные характеристики:

  Оценка сложности атаки следующая:

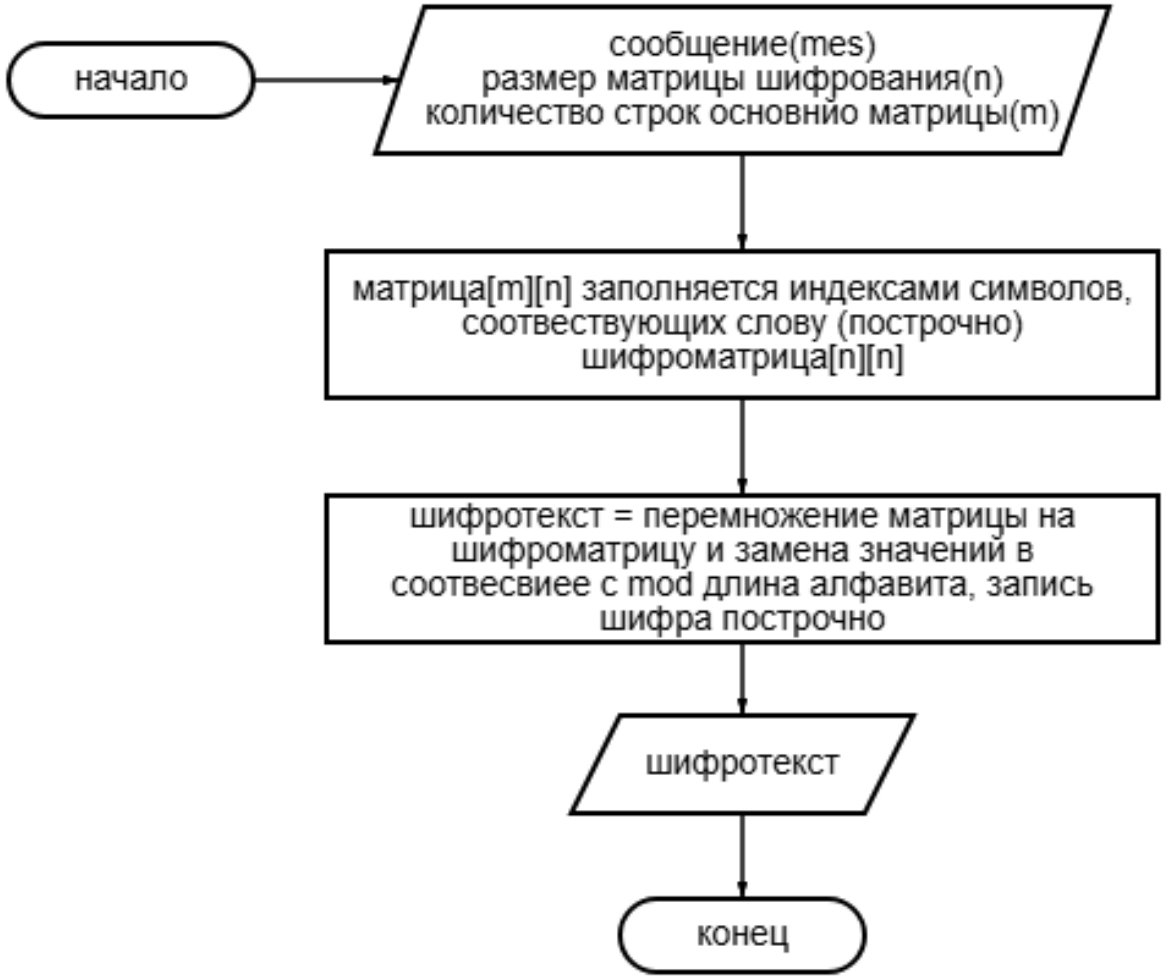
  $O\left(\frac{n!}{(n-m)!}\right)$, где n и m – мощность алфавита и длина кодового слова соответственно.

Шифр Хилла (Hill)

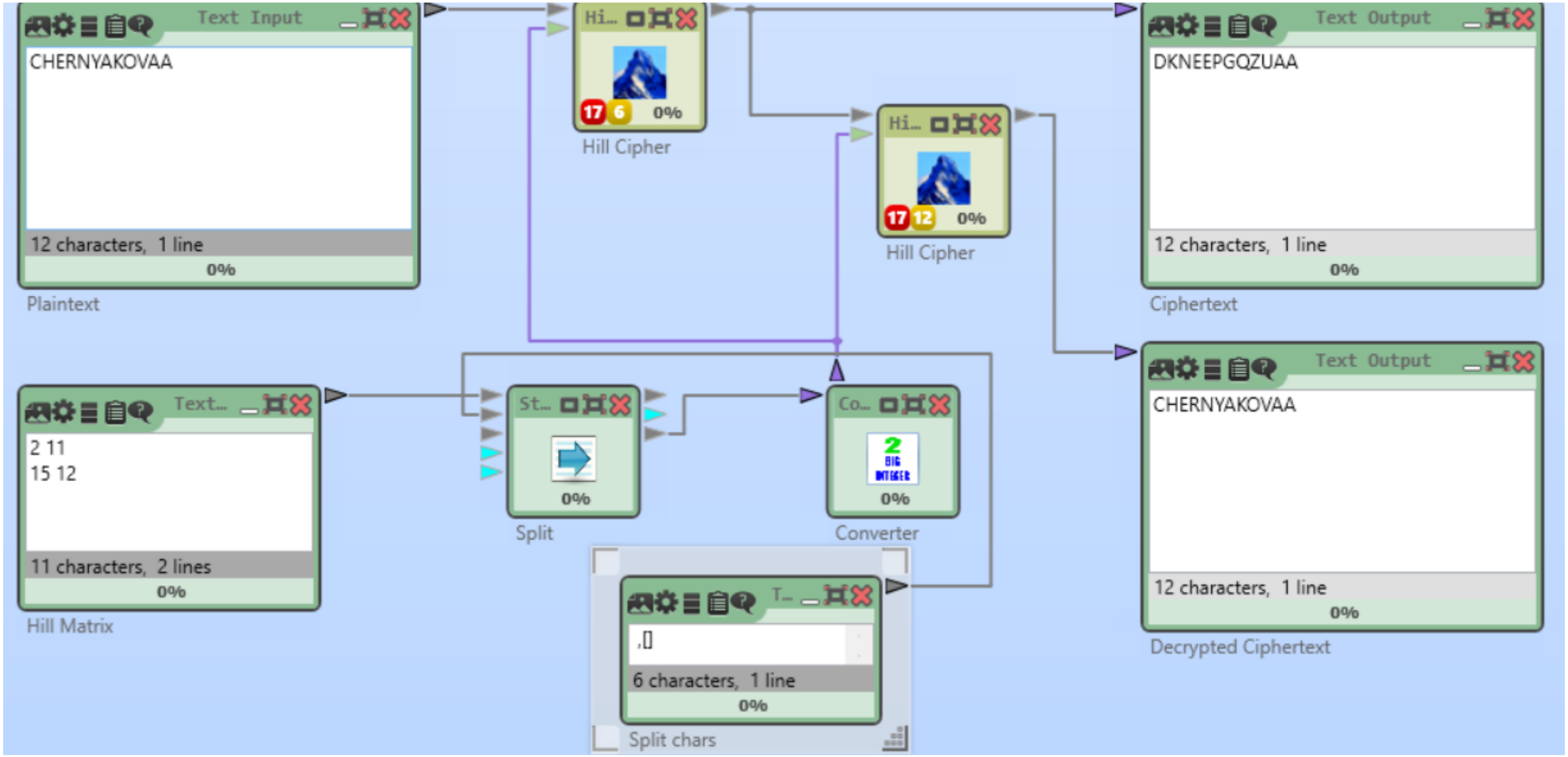
Задание

1. Найти шифр в CrypTool 2.
2. Зашифровать и расшифровать текст, содержащий только вашу фамилию (транслитерация латиницей), вручную и с помощью шифра с выбранным ключом 2 × 2. Убедиться в совпадении результатов. Проверить обратимость шифрующей матрицы (ключа).
3. Зашифровать текст с произвольным сообщением в формате «DEARMR ФАМИЛИЯ ИМЯ ОТЧЕСТВО THANK YOU VERY MUCH», используя транслитерацию латиницей и шифрующую матрицу 3 × 3.
4. Выполнить атаку на основе знания открытого текста, используя при ложение из Analysis –> Symmetric Encryption(classic) –> Known Plaintext.

Схема работы шифра



Шифрование и расшифровка фамилии



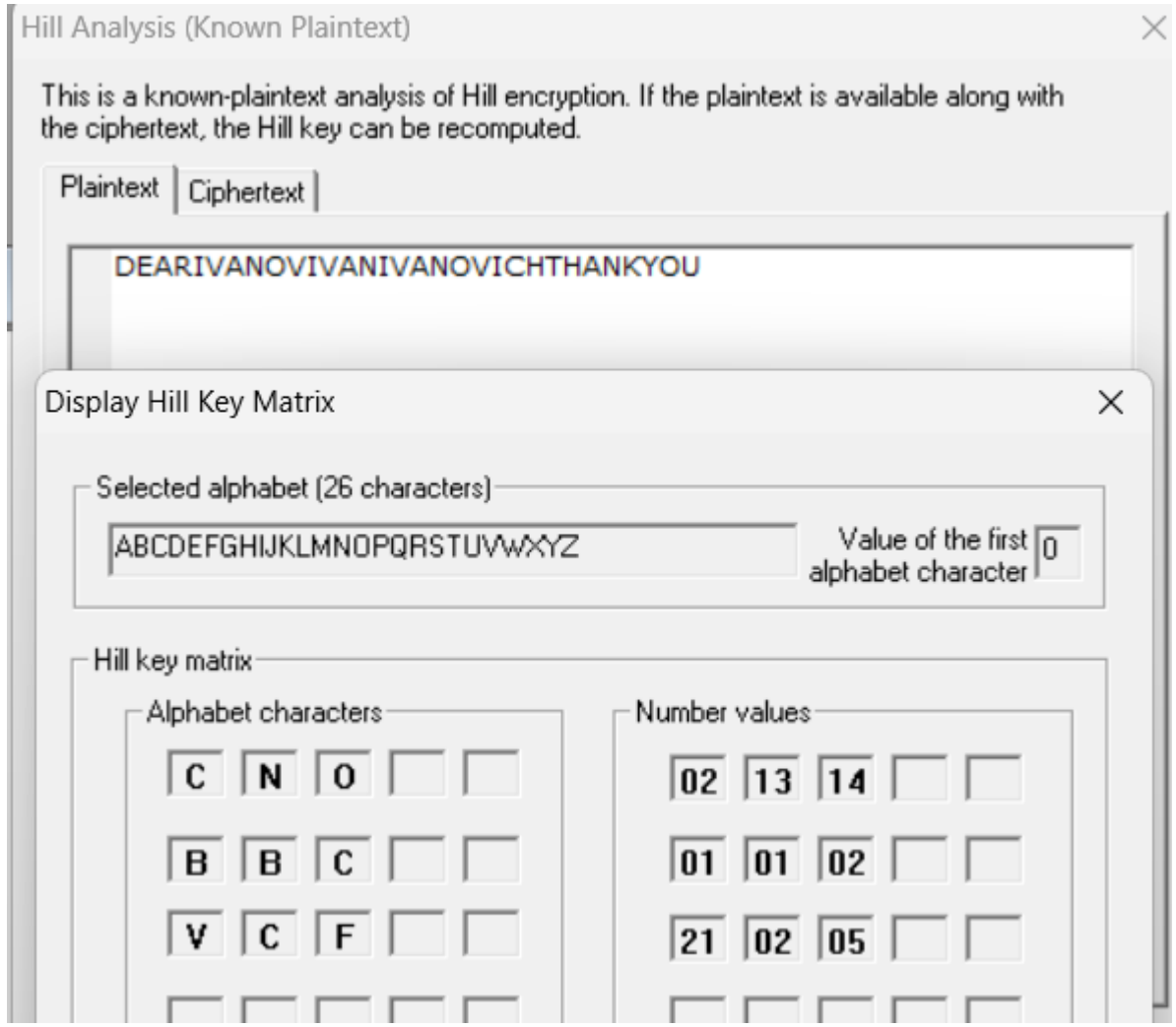
Шифрование и расшифровка фамилии

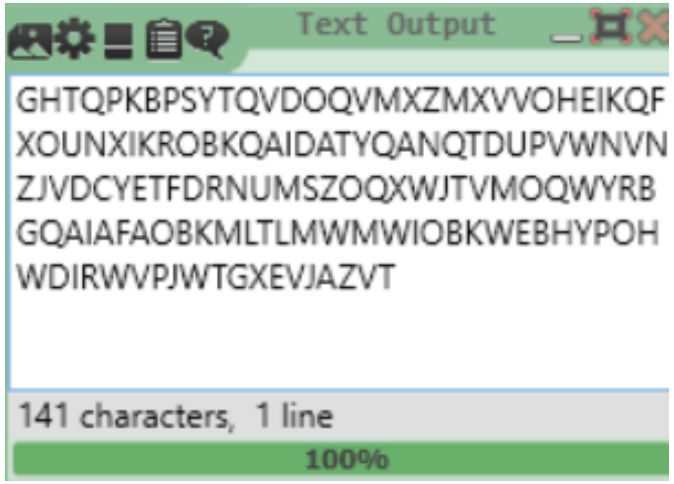
A	B	**C**	D	**E**	F	G	**H**	I	J	**K**	L	M	**N**	**O**	P	Q	**R**	S	T	U	**V**	W	X	**Y**	Z
0	1	**2**	3	**4**	5	6	**7**	8	9	**10**	11	12	**13**	**14**	15	16	**17**	18	19	20	**21**	22	23	**24**	25

C	H	=	2	7	×	2	15	=	81	114	mod 26 =	3	10	= DKNEEPGQZUAA											
E	R		4	17		11	12		195	264		13	4												
N	Y		13	24					290	483		4	15												
A	K		0	10					110	120		6	16												
O	V		14	21					259	462		25	20												
A	A		0	0					0	0		0	0												

D	K	=	3	10	×	6	25	=	28	215	mod 26 =	2	7	= CHERNYAKOVA											
N	E		13	4		1	14		82	381		4	17												
E	P		4	15					39	310		13	24												
G	Q		6	16					52	374		0	10												
Z	U		25	20					170	905		14	21												
A	A		0	0					0	0		0	0												

Атака на шифр





Заключение

- Изучен шифр Хилла и выявлены его следующие основные характеристики:

  Тип шифра – замена;

  Ключ шифра – шифрующая матрица.

- Проведена атака методом грубой силы на шифр Хилла и выявлены ее следующие основные характеристики:

  Оценка сложности атаки следующая:

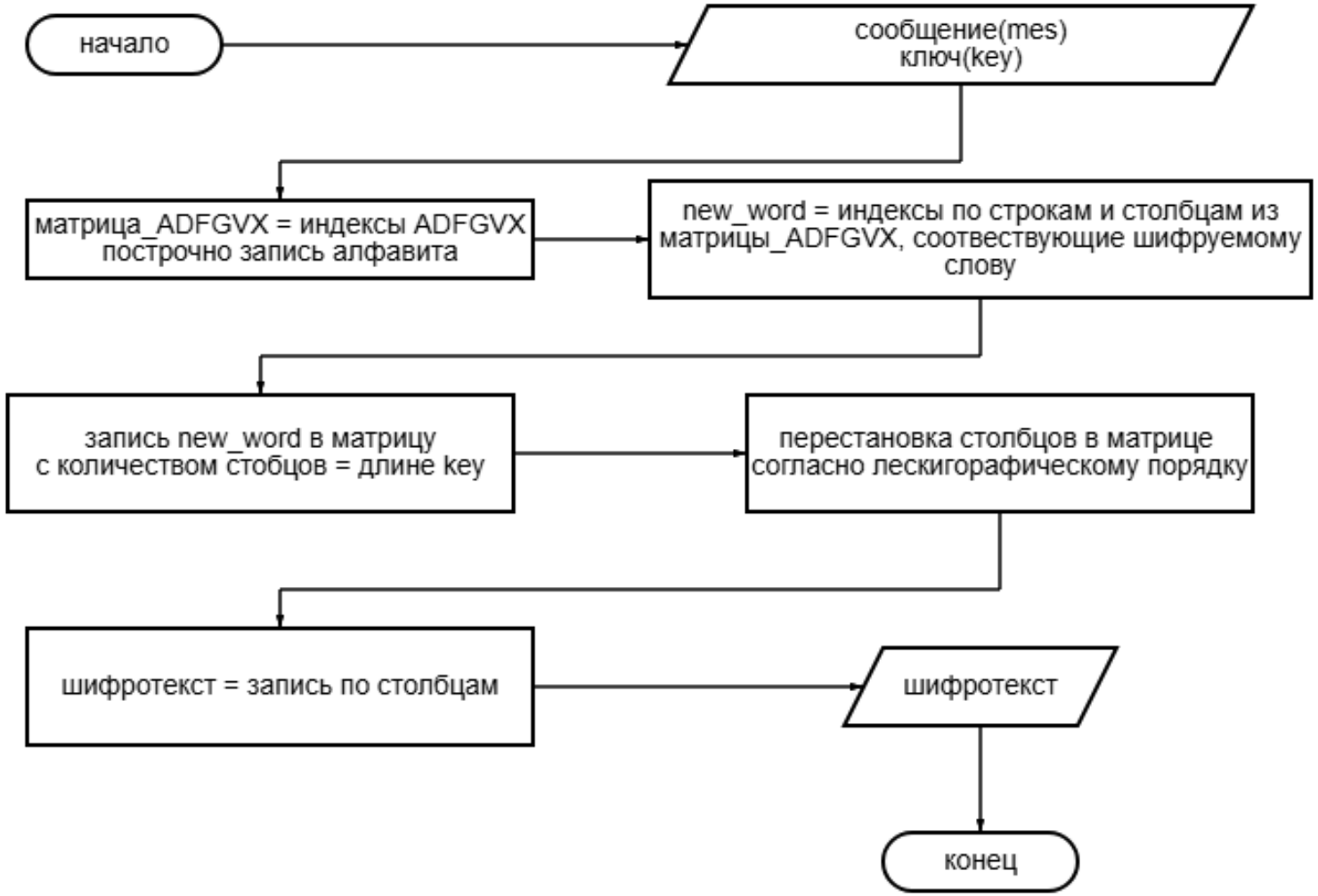
  $O(n^{m \times m})$, где n и m – мощность алфавита и размер матрицы соответственно.

Шифр ADFGVX

Задание

1. Найти шифр в CrypTool.
2. Зашифровать и расшифровать текст, содержащий только вашу фамилию (транслитерация латиницей), вручную и с помощью шифра с 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 150 символов.
6. Изучить инструмент автоматизации ручного расшифрования для текстов менее 300 символов.

Схема работы шифра



Работа шифра на фамилии

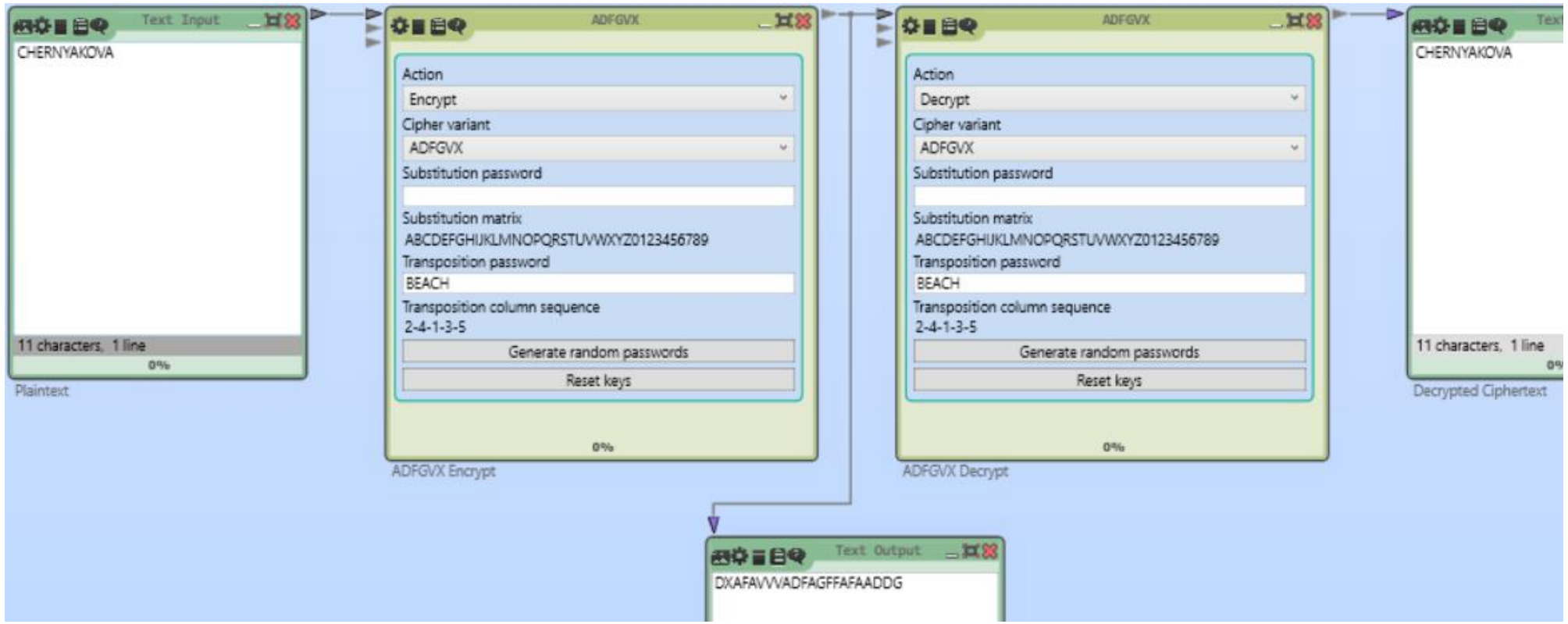
	A	D	F	G	V	X
A	A	B	C	D	E	F
D	G	H	I	J	K	L
F	M	N	O	P	Q	R
G	S	T	U	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

AFDDAVFXFDVAAADVFFGGAA

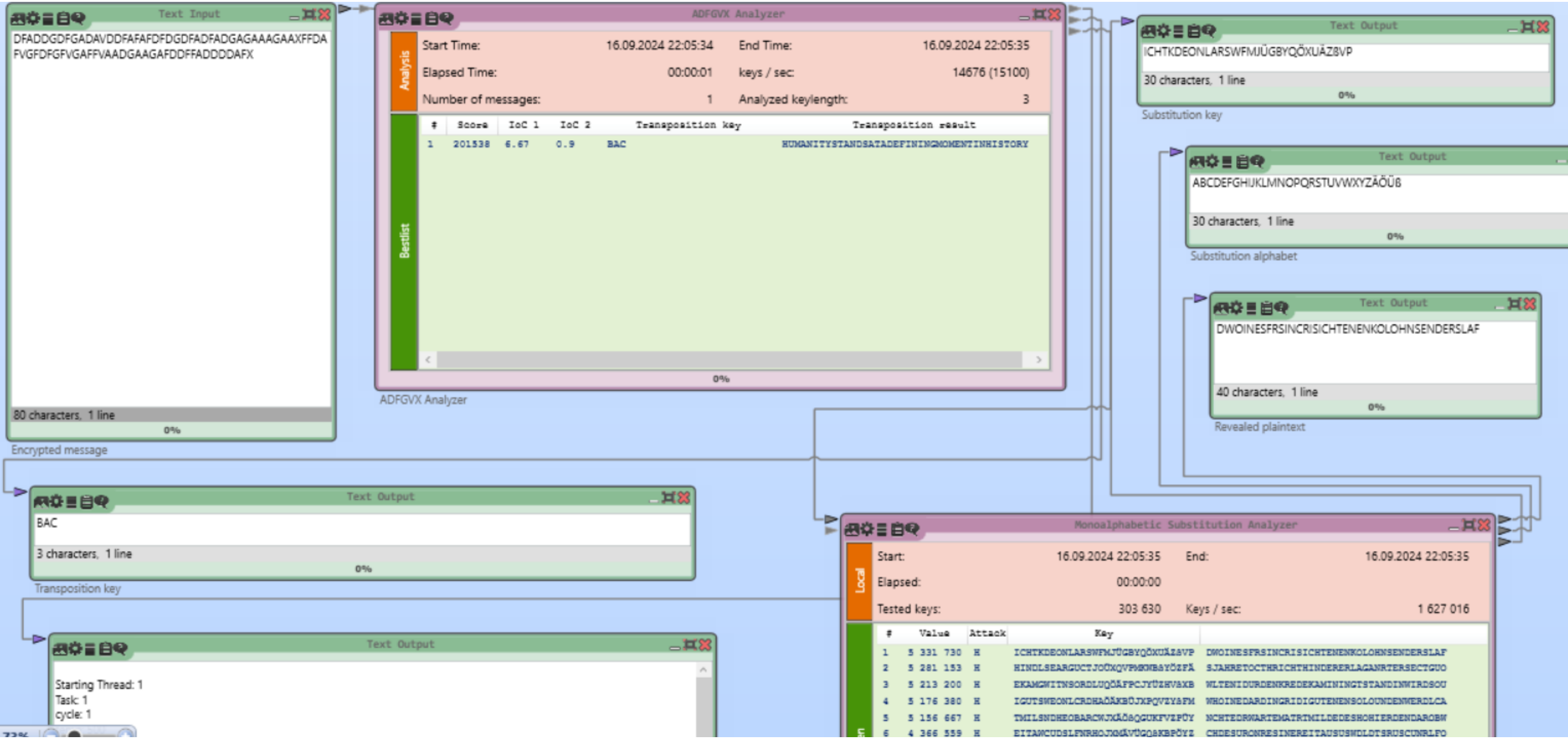
B	E	A	C	H
2	4	1	3	5
A	F	D	D	A
V	F	X	F	D
V	A	A	A	D
V	F	F	G	G
A	A			

A	B	C	E	H
1	2	3	4	5
D	A	D	F	A
X	V	F	F	D
A	V	A	A	D
F	V	G	F	G
	A		A	

DXAFAVVVADFAGFFAFAADDG



Атака на шифр



Заключение

- Изучен шифр ADFGVX и выявлены его следующие основные характеристики:

  Тип шифра – комбинированный, замена + перестановка;

  Ключ шифра – матрица + ключевое слово.

- Проведена атака методом грубой силы на шифр ADFGVX и выявлены ее следующие основные характеристики:

  Оценка сложности атаки следующая:

  $O(36! \times n!)$, где n – длина ключевого слова.