

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

Цель работы

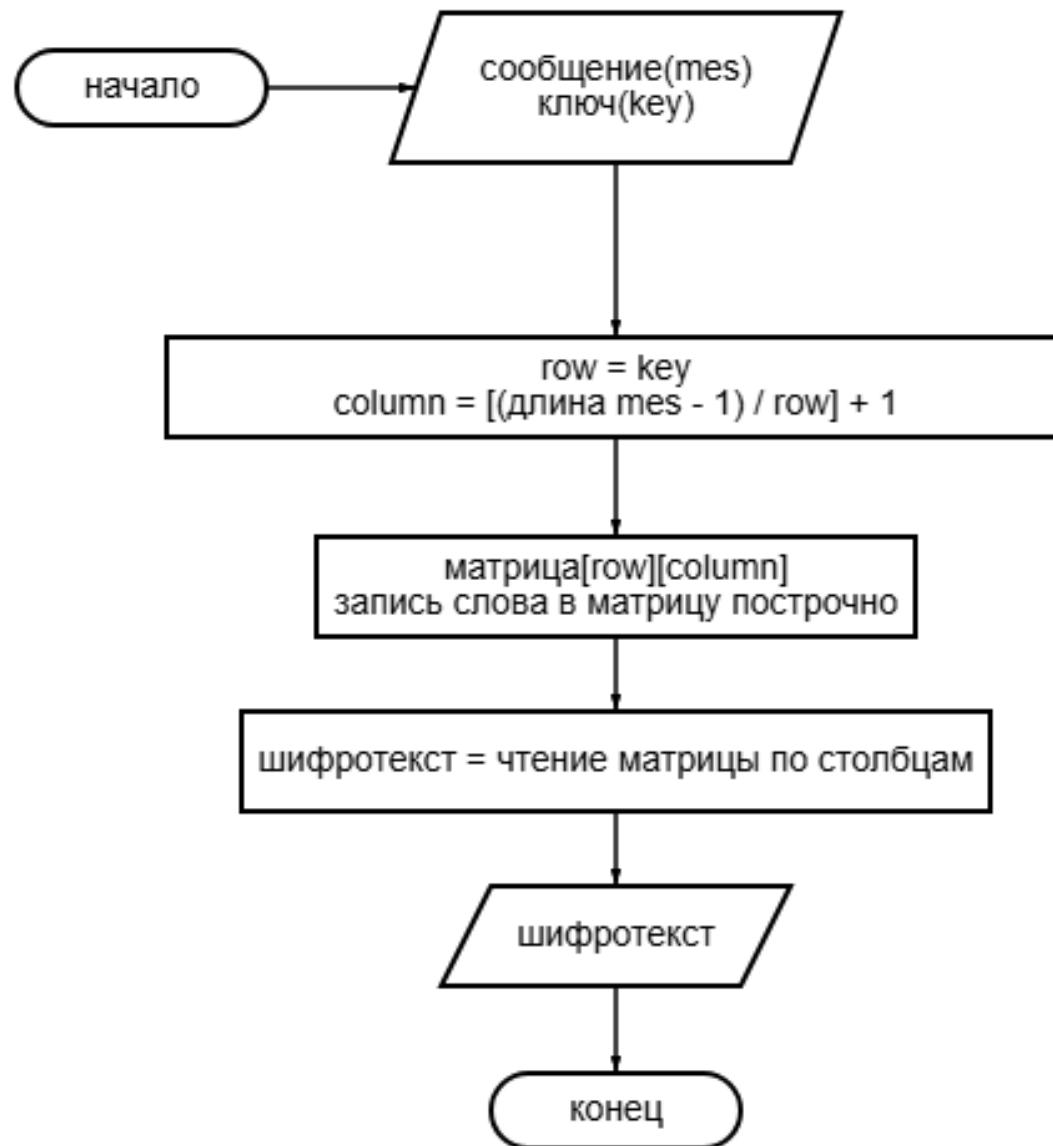
Исследовать шифры Scytale, Caesar, Substitution, Permutation/Transposition, Vigenere, Hill, ADFGVX и получить практические навыки работы с ними, в том числе с использованием приложений CrypTool 1 и 2.

Шифр «Сцитала» (Scytale)

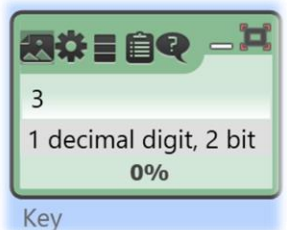
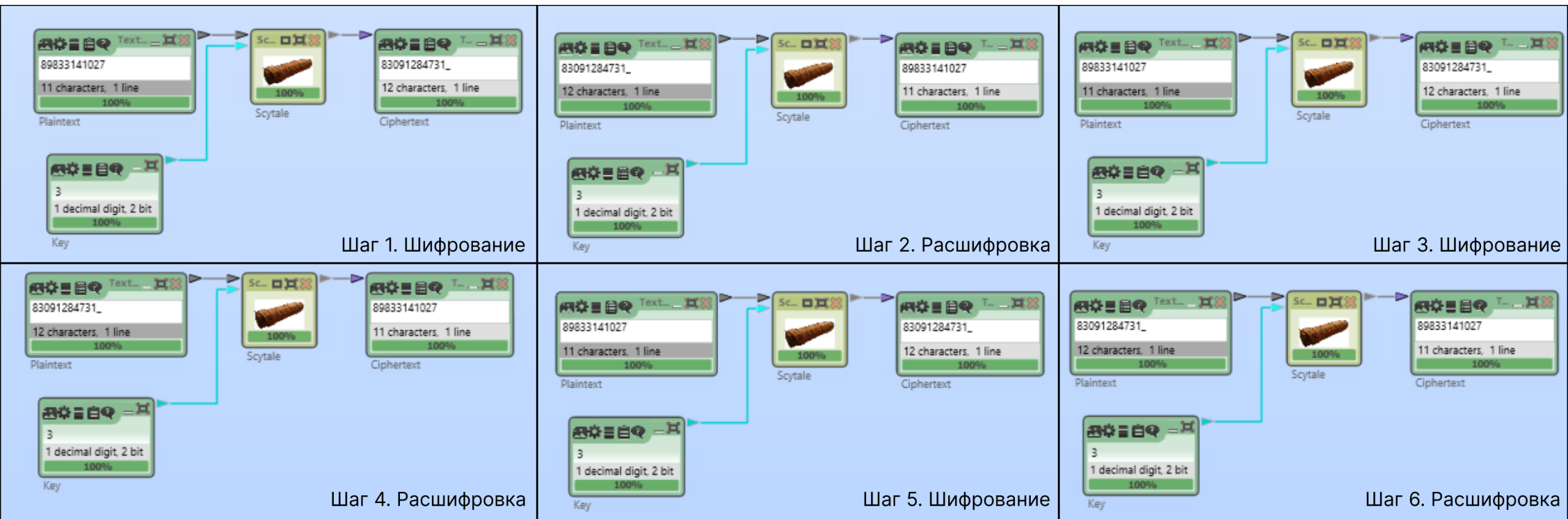
Задание

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 \geq 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



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 _

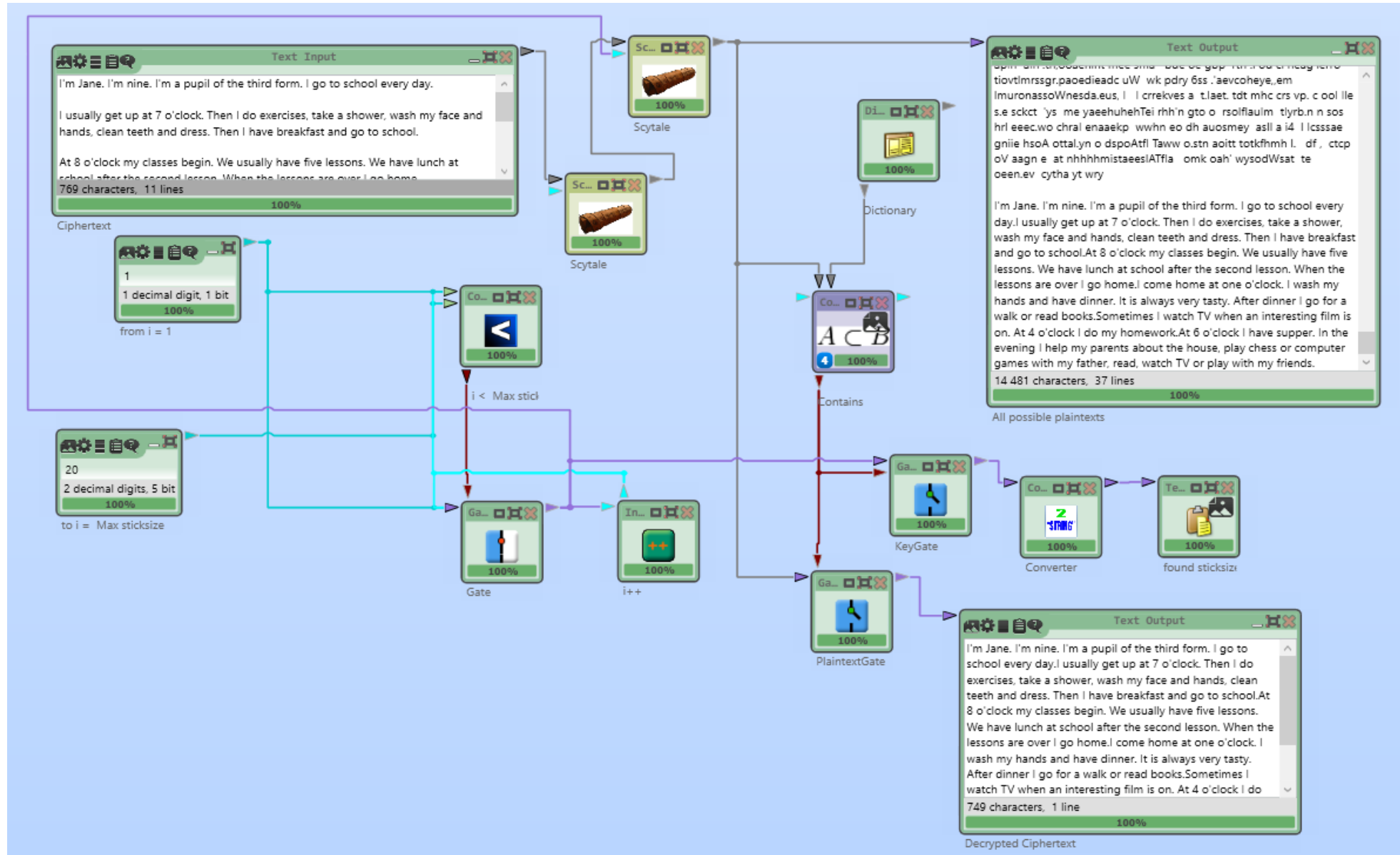
CHERNYAKOVA

С применением CrypTool2

Number of Edges = 4



Атака на шифр методом «грубой силы»



Заключение

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

Тип шифра – перестановка;

Ключ шифра – количество граней цилиндра.

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

Оценка сложности атаки следующая:

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

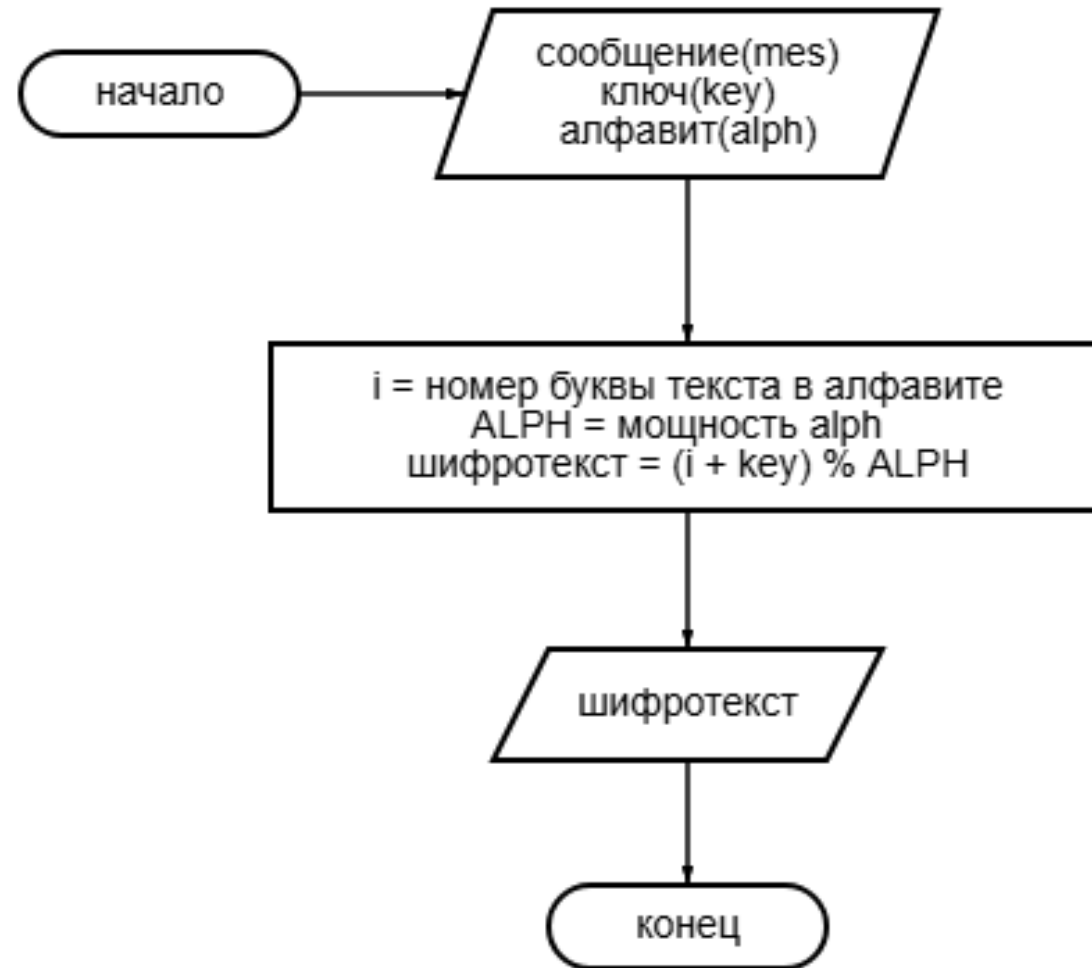
$O(n^2)$, когда используется смещение.

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

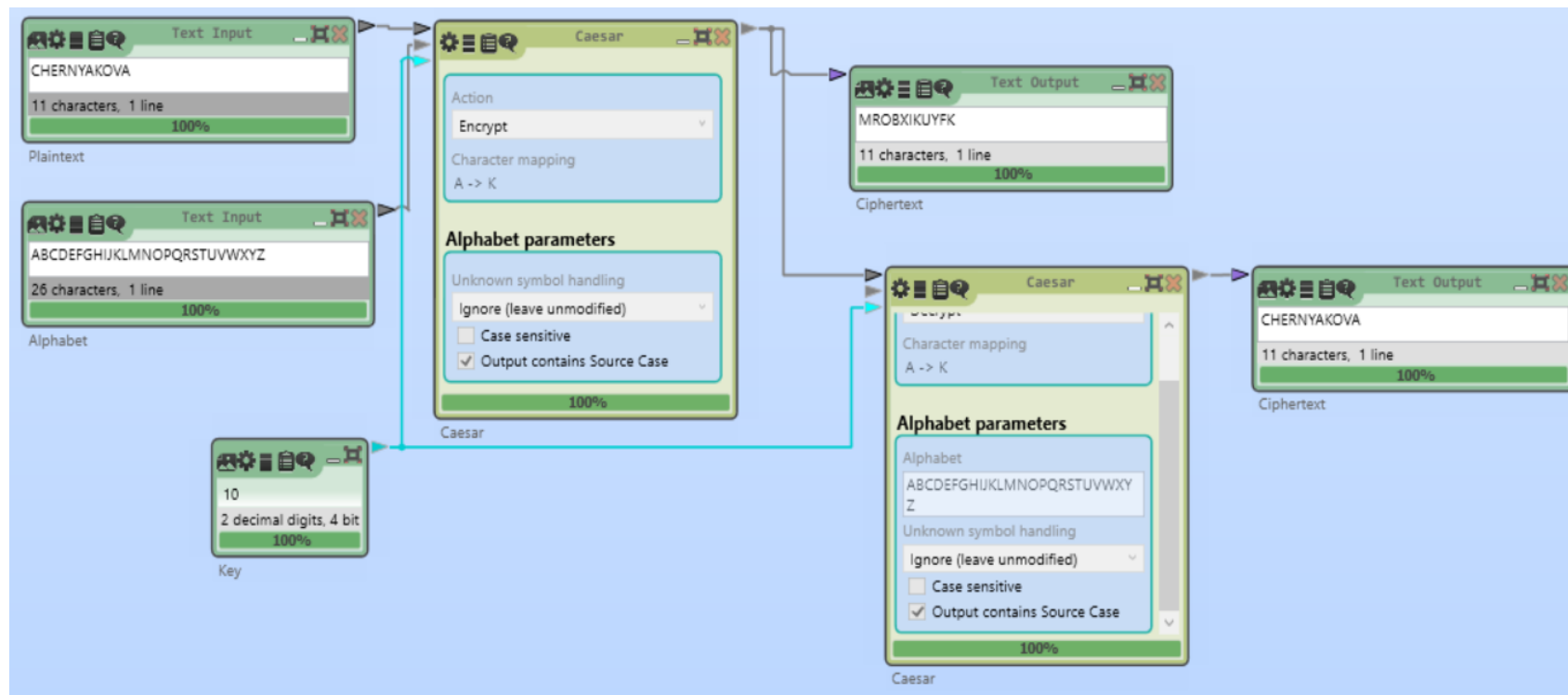
MROBXIKUYFK

ABCDEFGHIJKLMNOPQRSTUVWXYZ
KLMNOPQRSTUVWXYZABCDEFGHIJ

CHERNYAKOVA

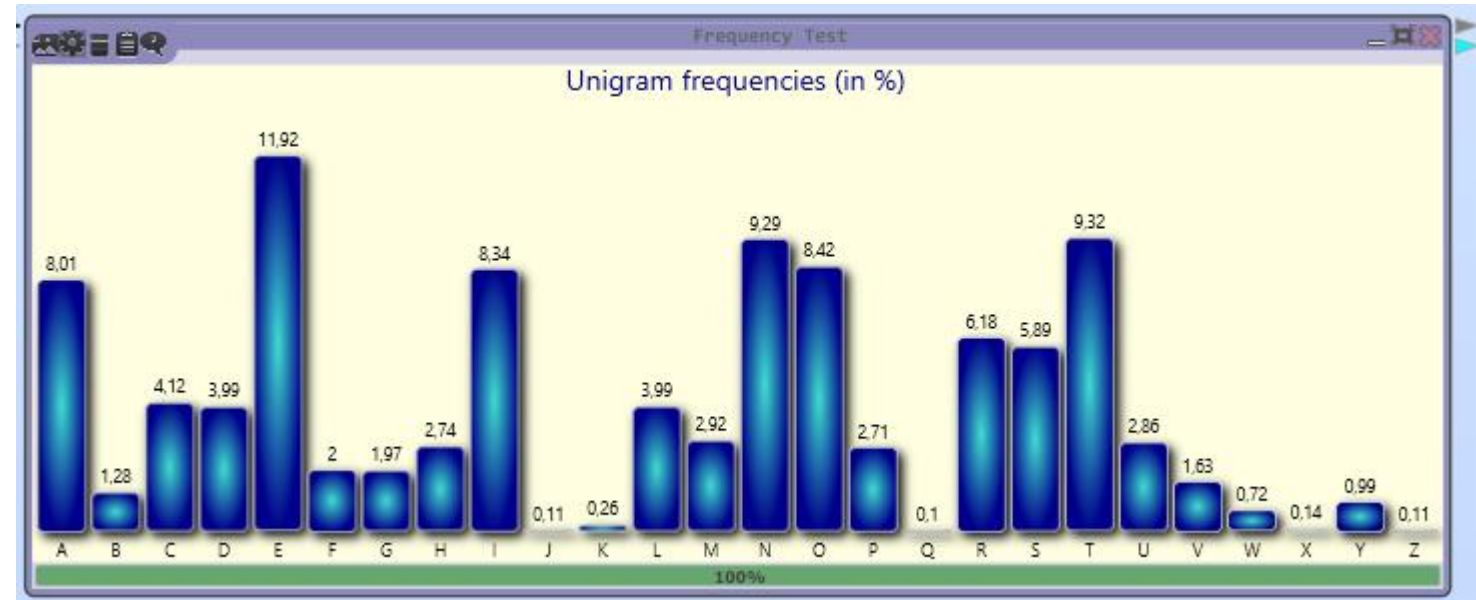
С применением CrypTool2

Key = 10

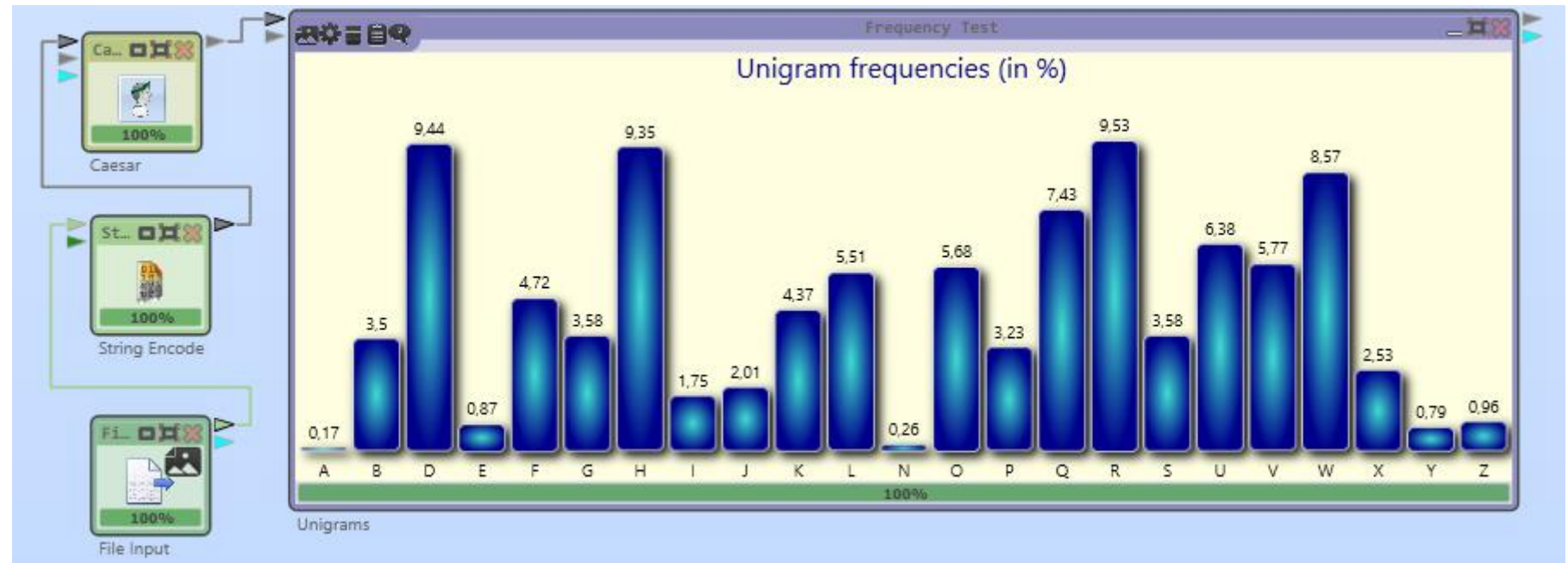


Сравнения гистограмм частот символом

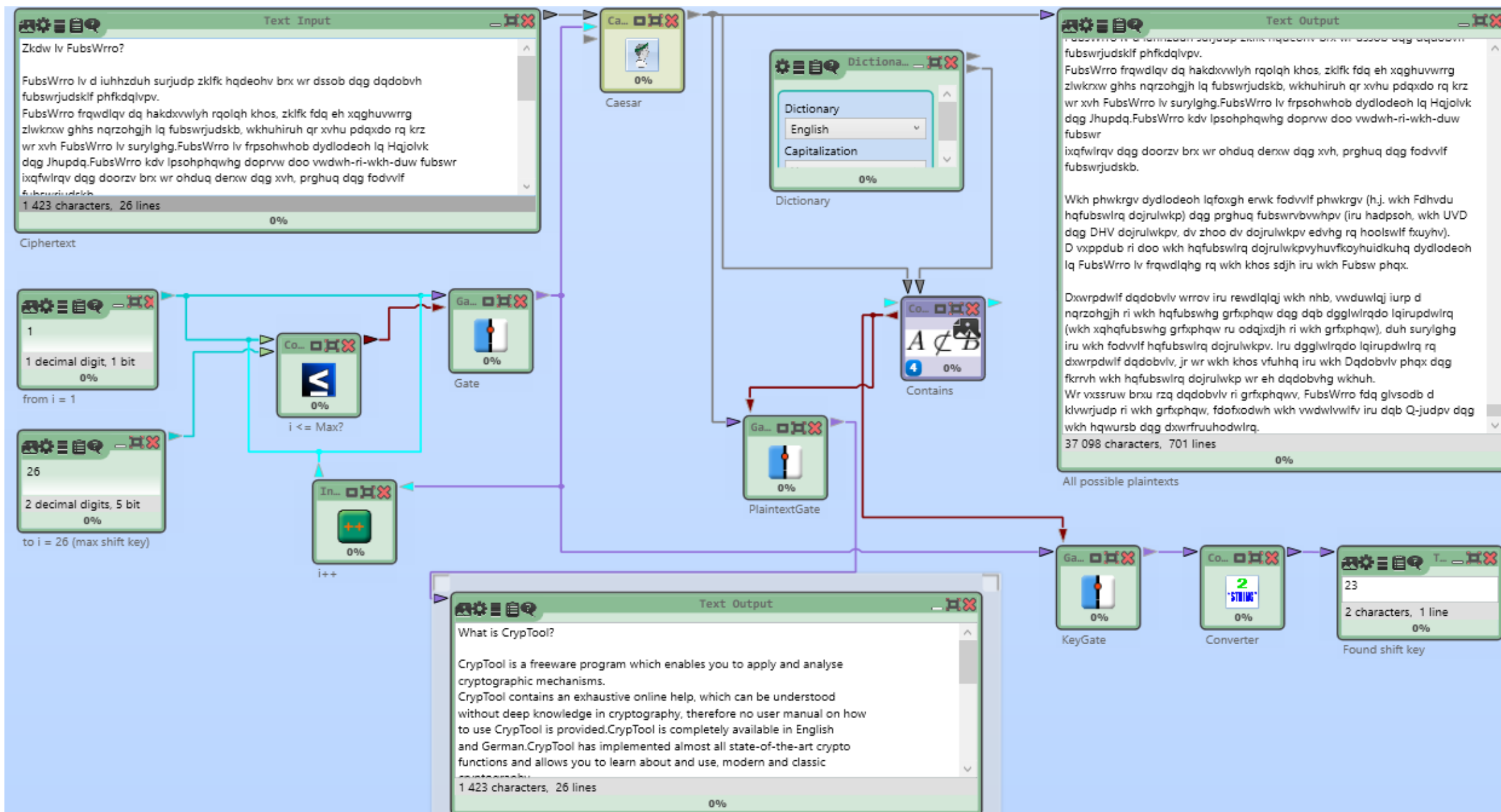
Файл *CrypTool-en.txt* был зашифрован с ключом $key = 3$. То есть $A \rightarrow D$. Гистограмма представлена снизу. Справа представлена гистограмма текста *English.txt*.



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

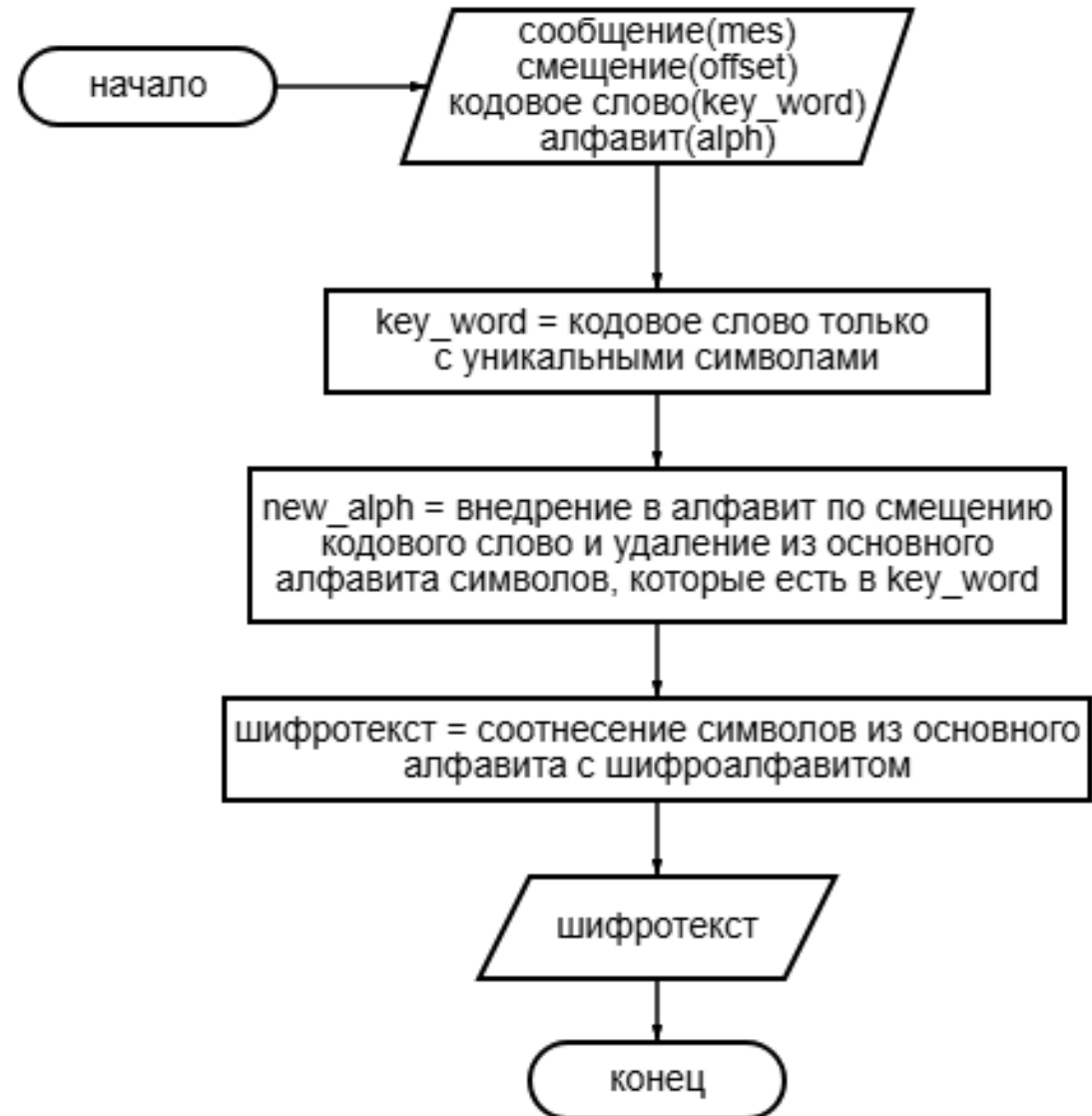
- Изучен шифр Цезаря и выявлены его следующие основные характеристики:
 - Тип шифра – замена;
 - Ключ шифра – смещение по алфавиту.
- Проведена атака методом грубой силы на шифр Цезаря и выявлены ее следующие основные характеристики:
 - Оценка сложности атаки следующая:
 - $O(n)$, где n – мощность алфавита.

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 $\neq 0$. 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

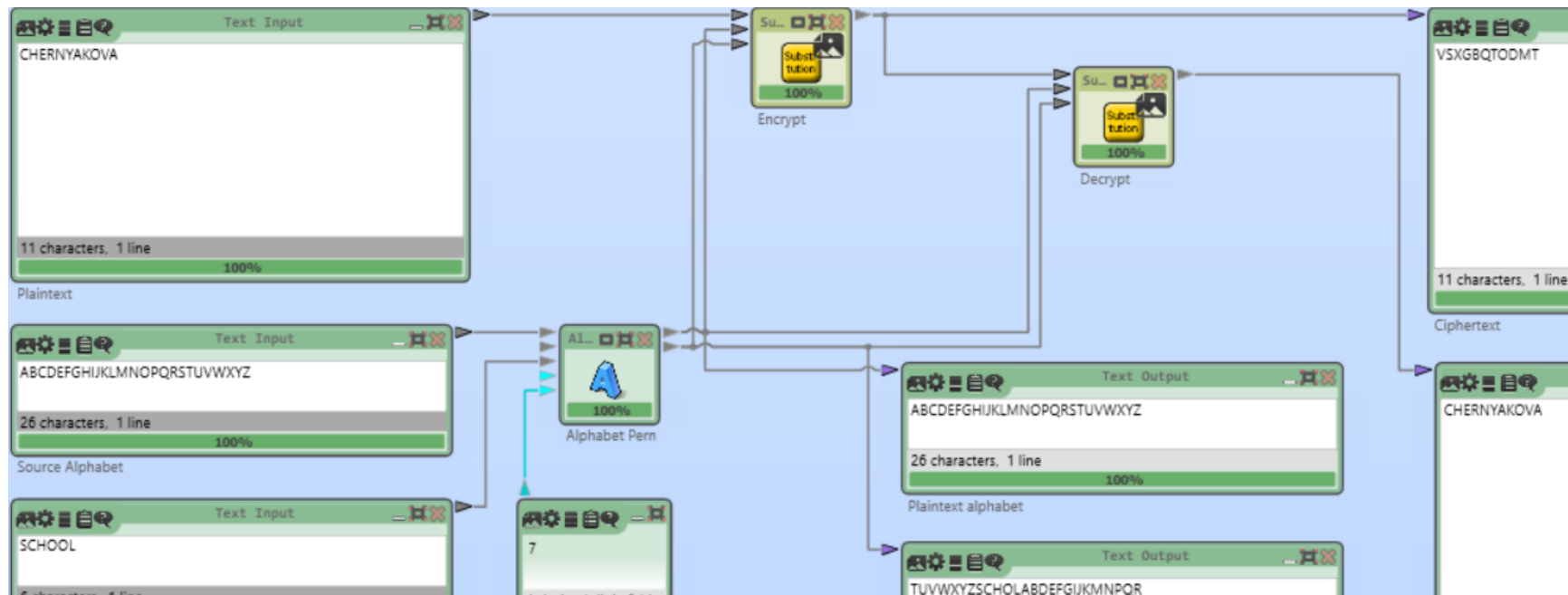
Key = SCHOOL, Offset = 7

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

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

The screenshot displays the Monoalphabetic Substitution Analyzer interface. The 'Text Input' window on the left contains a 600-character ciphertext. The central window shows the cryptanalysis results, including the start and end times, elapsed time, and the number of tested keys. The 'Top Ten' table lists the top candidates, with the first candidate being the correct plaintext. The 'Text Output' window on the right displays the decrypted text.

Text Input

PAAPJZHUWQ, UDX JYZ WEDJPKDPDR
XZJZHPEHUJED EC JYZ ZWEIQIZBI ED MYPWY
MZ XZFZDX CEH EKH
MZAA-VZPDR, YEMZLZH, PDJZRHUJED EC
ZDLPHEDBZDJ UDX XZLZAEFBZDJ WEDWZHD
UDX RHZUJZH
UJJZDPED JE JYZB MPAA AZUX JE JYZ
CKACPABZDJ EC VUIPW DZZXI, PBFHELZX
APLPDR IJUDXUHXI CEH
UAA, VZJZH FHEJZWJZX UDX BUDURZX
ZWEIQIZBI UDX U IUCZH, BEHZ FHEIFZHEKI
CKJKHZ, DE DUJED
WUD UWYPZLZ JYPI ED PJI EMD; VKJ JERZJYZH
MZ WUD - PD U RAEVUA FUHJDZHIYPF CEH
IKIUPDUVAZ
XZLZAEFBZDJ.
653 characters, 8 lines
0%

Monoalphabetic Substitution Analyzer

Start: 15.09.2024 16:49:57 End: 15.09.2024 16:49:58
Elapsed: 00:00:00
Tested keys: 32 292 Keys / sec: 126 995

#	Value	Attack	Key
1	4 485 980	H	YJQXLMFNOPRSTUVWIKGABCDHE Z HUMANITK STANDS AT A DEFINING MOMENT IN HISTORKQ W
2	2 676 338	H	BJWZFLDA PSMRUHGOYKTKXNVCEIQ CULTAORYIMRTAVMITRITIVEDOAOAKIL LEARIOAICOMR SYWIG

Text Output

HUMANITK STANDS AT A DEFINING MOMENT
IN HISTORKQ WE ARE CONFRONTED WITH A
PERPETUATION OF DISPARITIES BETWEEN AND
WITHIN NATIONS A WORSENING OF
POVERTKY HUNGERY ILL HEALTH AND
ILLITERACKY AND THE CONTINUING
DETERIORATION OF THE ECOSKSTEMS ON
WHICH WE DEPEND FOR OUR WELLJBEINGQ
HOWEVERY INTEGRATION OF ENVIRONMENT
AND DEVELOPMENT CONCERNS AND GREATER
ATTENTION TO THEM WILL LEAD TO THE
FULFILMENT OF BASIC NEEDSY IMPROVED
LIVING STANDARDS FOR ALLY BETTER
PROTECTED AND MANAGED ECOSKSTEMS AND
A SAFERY MORE PROSPEROUS FUTUREQ NO
NATION CAN ACHIEVE THIS ON ITS OWNX BUT
639 characters, 1 line
0%

Input of the ciphertext Cryptanalysis of the ciphertext. Different plaintext candidates and the according keys are shown. Output of the plaintext

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

The screenshot displays the Monoalphabetic Substitution Analyzer interface. The 'Text Input' window on the left contains a 300-character ciphertext. The central window shows the cryptanalysis results, including the start and end times, elapsed time, and the number of tested keys. The 'Top Ten' table lists the top candidates, with the first candidate being the correct plaintext. The 'Text Output' window on the right displays the decrypted text.

Text Input

YKBUDPJQ IJUDXI UJ U XZCPDPDR BEBZDJ PD
YPIEHQ, MZ UHZ WEDCHEDJZX MPJY U
FZHFZJKUJED EC XPIFUHPJZI VZJMZZD UDX
MPJYPD DUJEDI, U MEHIZDPDR EC FELZHIQ,
YKDRZH, PAA YZUAJY UDX PAAPJZHUWQ, UDX JYZ
WEDJPKDPDR XZJZHPEHUJED EC JYZ ZWEIQIZBI
ED MYPWY MZ XZFZDX CEH EKH MZAA-VZPDR,
YEMZLZH, PDJZRHUJED.

Monoalphabetic Substitution Analyzer

Start: 15.09.2024 16:52:59 End: 15.09.2024 16:52:59
Elapsed: 00:00:00
Tested keys: 30 888 Keys / sec: 217 912

#	Value	Attack	Key
1	4 489 967	H	KJQLMFNOPRSTUVWIKGABCDHE XZ HUMANITY STANDS AT A DEFINING MOMENT IN HISTORYQ W
2	2 937 542	H	MQYKWR TCOHIDGUSXBLVFPNEAJZ NDWL SIXAHIL PHALIALAPERS S BAWTWE IAS ANSHITOKYAU

Text Output

HUMANITY STANDS AT A DEFINING MOMENT IN
HISTORYQ WE ARE CONFRONTED WITH A
PERPETUATION OF DISPARITIES BETWEEN AND
WITHIN NATIONSK A WORSENING OF POVERTYK
HUNGERK ILL HEALTH AND ILLITERACYK AND THE
CONTINUING DETERIORATION OF THE
ECOSYSTEMS ON WHICH WE DEPEND FOR OUR
WELLJBEINGQ HOWEVERK INTEGRATIONQ

Атака на шифр

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

YKBUDPJQ IJUDXI UJ U XZCPDPDR BEBZDJ PD
YPIEHQ. MZ UHZ WEDCHEDJZX MPJY U
FZHFZJKUJPD EC XPIFUHPJZI VZJMZZD UDX
MPJYPD DUJPEI, U MEHIZDPDR EC FELZHJQ.

Local

Start: 15.09.2024 16:55:40 End: 15.09.2024 16:55:40
Elapsed: 00:00:00
Tested keys: 29 484 Keys / sec: 376 799

#	Value	Attack	Key
1	4 601 707	H	KQLZMFNOPRSTUVWYIAGABCDHE JX
2	3 130 916	H	KQBJUD NGOLTHFRIMWSCVPYEAKZ
3	2 932 061	H	LJYXPUTADRI WBGSMZEFCHKONQV

HUMANITY STANDS AT A DEFINING MOMENT IN
HISTORYL WE ARE CONFRONTED WITH A
PERPETUATION OF DISPARITIES BETWEEN AND
WITHIN NATIONSK A WORSENING OF POVERTYL

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

Substitution Analysis: Manual Post-Processing

In this dialog window ciphertext characters are shown in small letters and plaintext characters are shown in capital letters (example: a -> C means that the letter 'a' is decrypted into 'C'). Each change of the substitution list below will result into a change of the intermediate status of decryption below. Using the actual state of decryption you may try out other substitutions.

a: <input type="text" value="S"/>	b: <input type="text" value="F"/>	c: <input type="text" value="L"/>	d: <input type="text" value="B"/>	e: <input type="text" value="U"/>	f: <input type="text" value="R"/>	g: <input type="text" value="K"/>
h: <input type="text" value="P"/>	i: <input type="text" value="E"/>	j: <input type="text" value="A"/>	k: <input type="text" value="H"/>	l: <input type="text" value="W"/>	m: <input type="text" value="T"/>	n: <input type="text" value="D"/>
o: <input type="text" value="J"/>	p: <input type="text" value="N"/>	q: <input type="text" value="I"/>	r: <input type="text" value="V"/>	s: <input type="text" value="M"/>	t: <input type="text" value="Z"/>	u: <input type="text" value="G"/>
v: <input type="text" value="O"/>	w: <input type="text" value="X"/>	x: <input type="text" value="Y"/>	y: <input type="text" value="C"/>	z: <input type="text" value="Q"/>		

Reset entries to the result of the automatic analysis

Current intermediate status of decryption:

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:

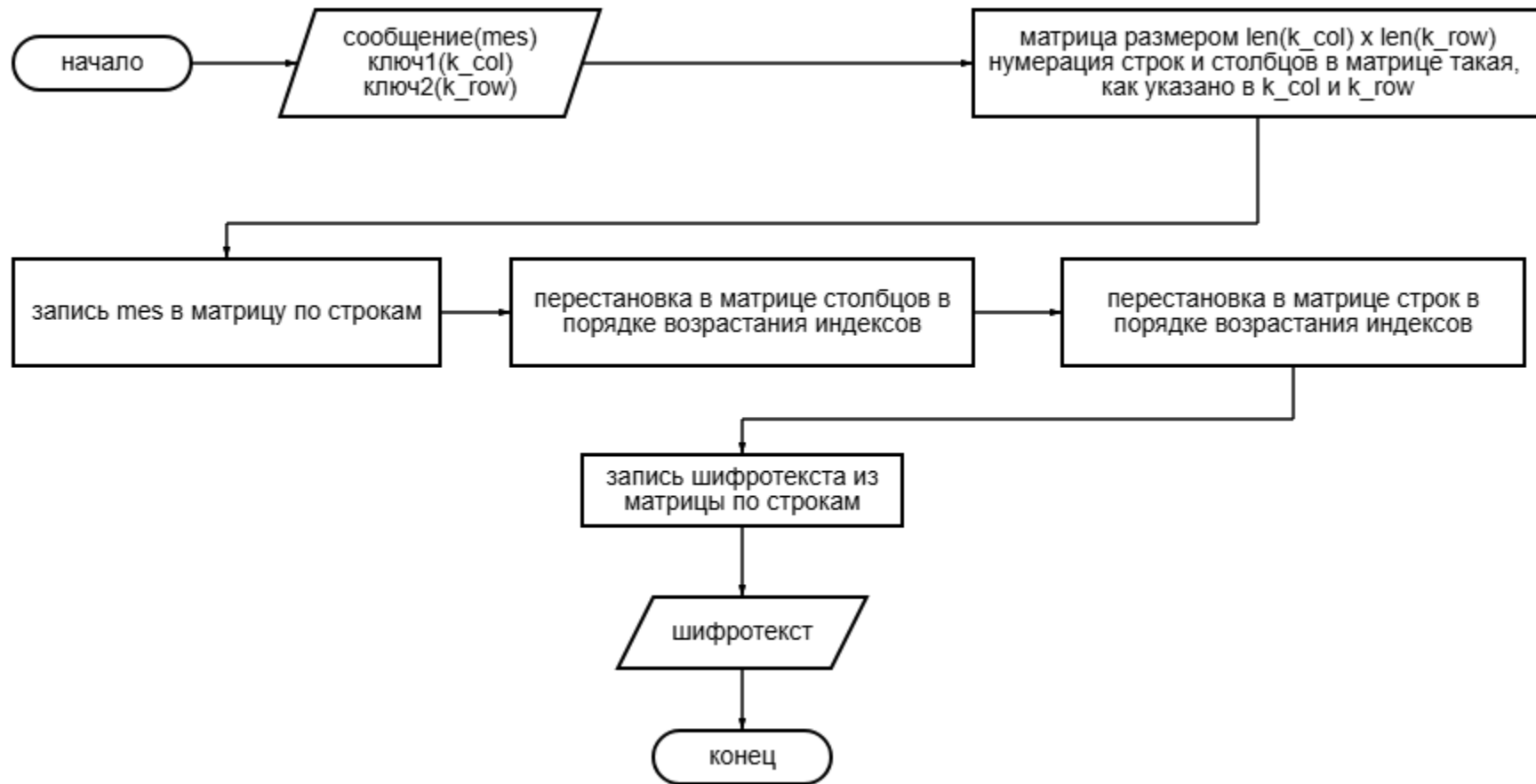
$O(n!)$, где n – мощность алфавита.

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 Plaintext.

Схема работы шифра



Шифрование и расшифровка ФИО

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

Вручную

ChernyakovaValeriyaAlekseevna

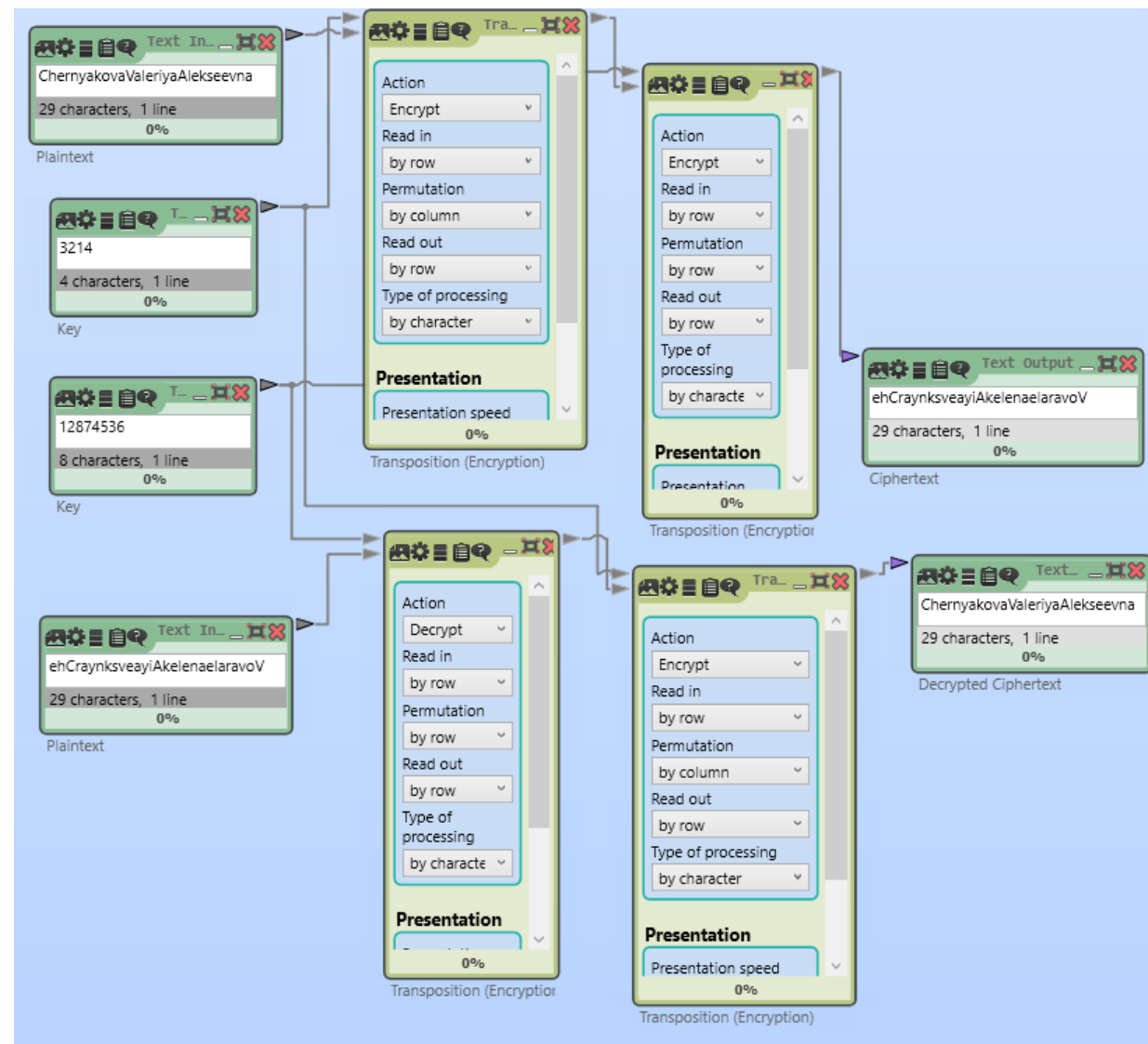
	3	2	1	4		1	2	3	4		1	2	3	4		
1	C	h	e	r		1	e	h	C	r		1	e	h	C	r
2	n	y	a	k		2	a	y	n	k		2	a	y	n	k
8	o	v	a	V		8	a	v	o	V		3	v	e	e	n
7	a	l	e	r		7	e	l	a	r		4	a	y	i	A
4	i	y	a	A		4	a	y	i	A		5	k	e	l	s
5	l	e	k	s		5	k	e	l	s		6			a	
3	e	e	v	n		3	v	e	e	n		7	e	l	a	r
6	a					6			a			8	a	v	o	V

ehCraynkveenayiAkels__a_elaravoV

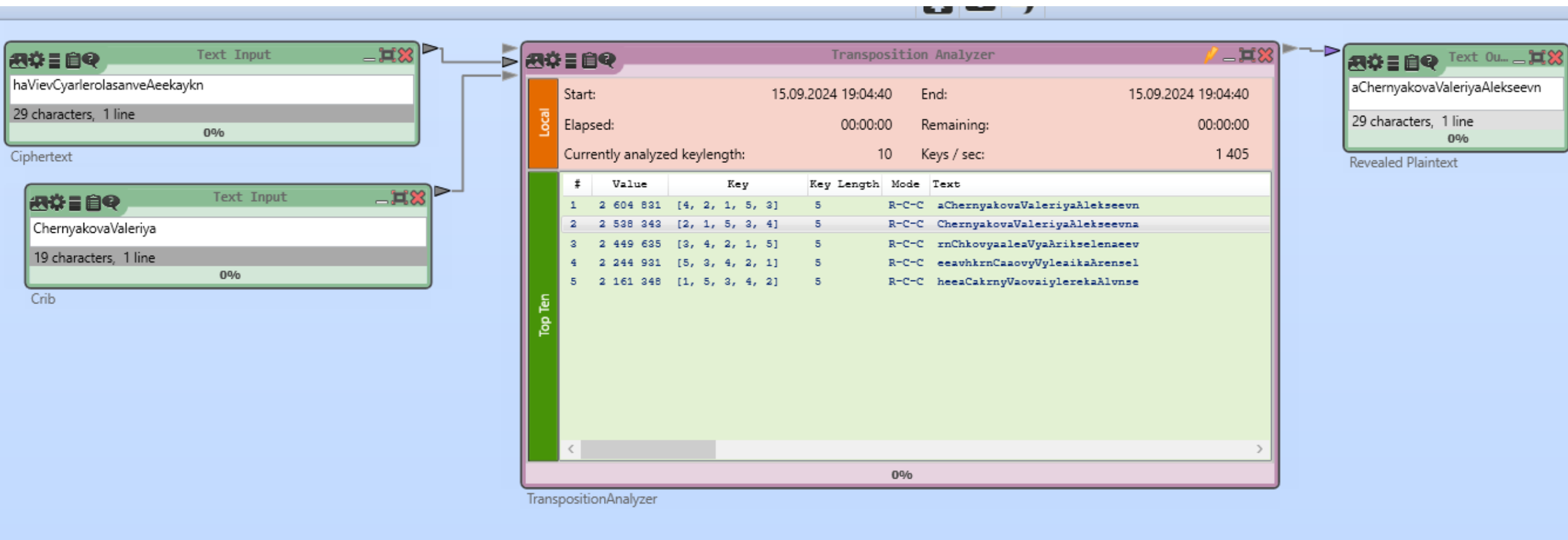
	1	2	3	4		1	2	3	4		3	2	1	4		
1	e	h	C	r		1	e	h	C	r		1	C	h	e	r
2	a	y	n	k		2	a	y	n	k		2	n	y	a	k
3	v	e	e	n		8	a	v	o	V		8	o	v	a	V
4	a	y	i	A		7	e	l	a	r		7	a	l	e	r
5	k	e	l	s		4	a	y	i	A		4	i	y	a	A
6			a			5	k	e	l	s		5	l	e	k	s
7	e	l	a	r		3	v	e	e	n		3	e	e	v	n
8	a	v	o	V		6			a			6			a	

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:

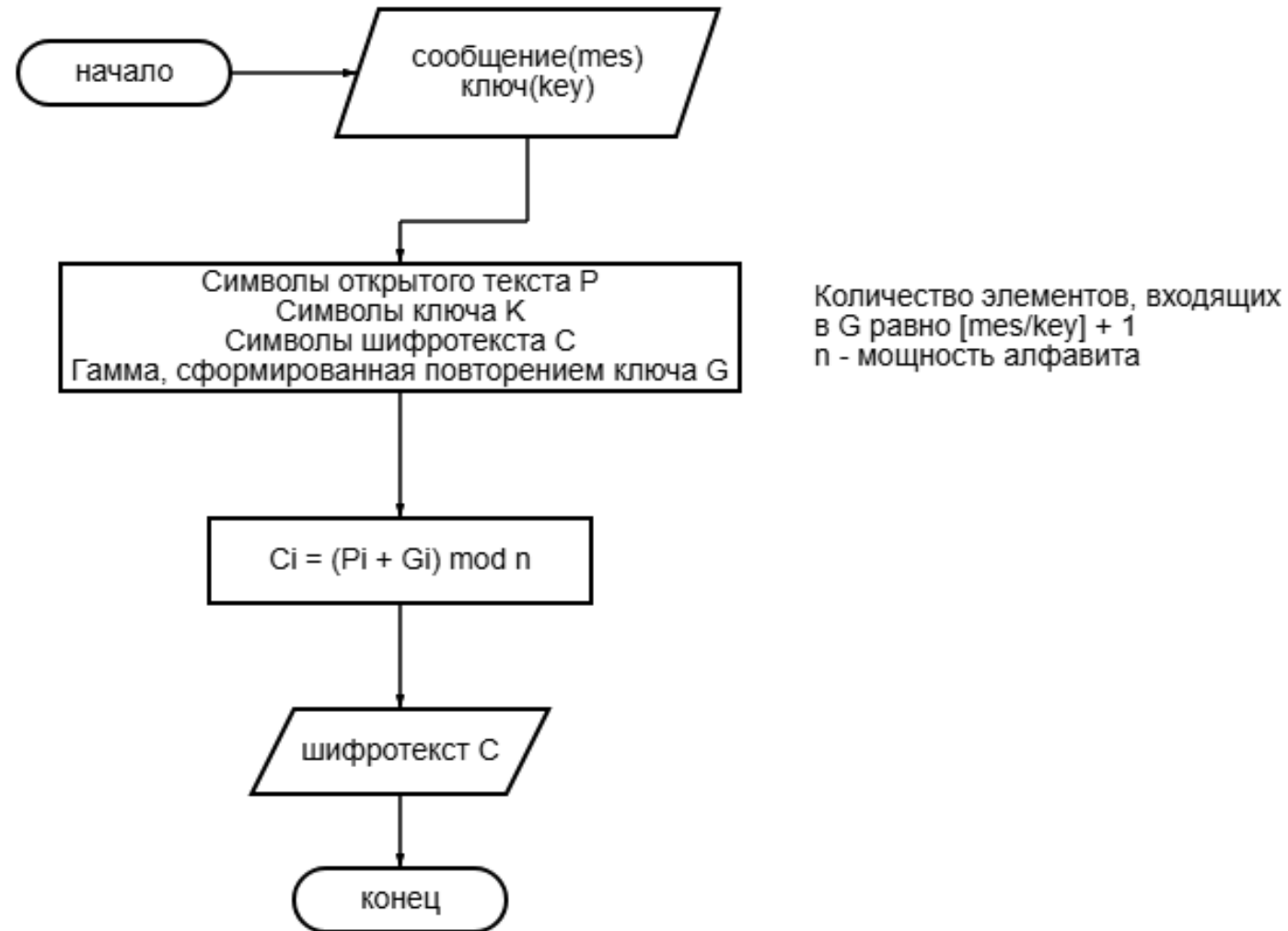
$O(n! * m!)$, где n и m – количество строк и столбцов матрицы.

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



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

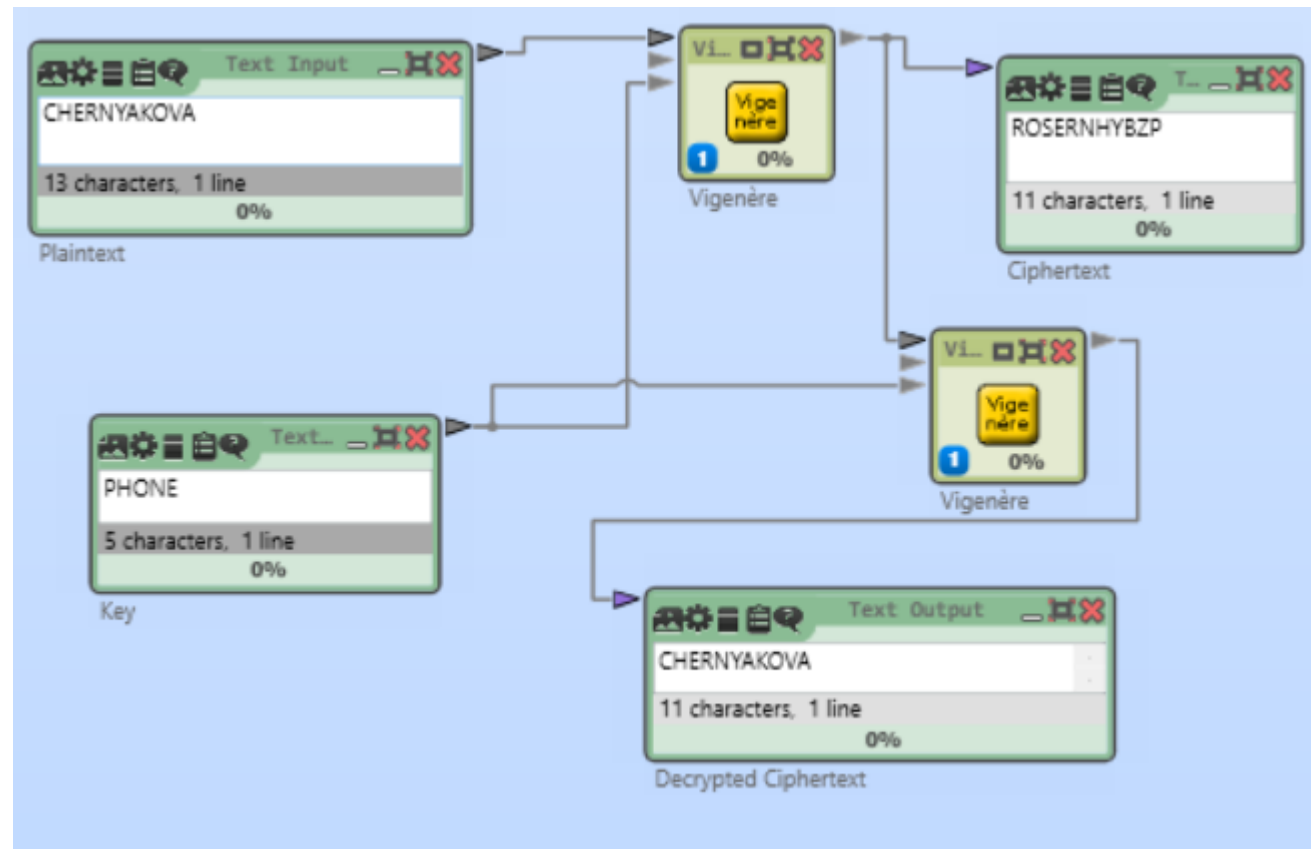
C	H	E	R	N	Y	A	K	O	V	A				
P	H	O	N	E	P	H	O	N	E	P	H	O	N	E
R	O	S	E	R	N	H	Y	B	Z	P				

ROSERNHYZBP

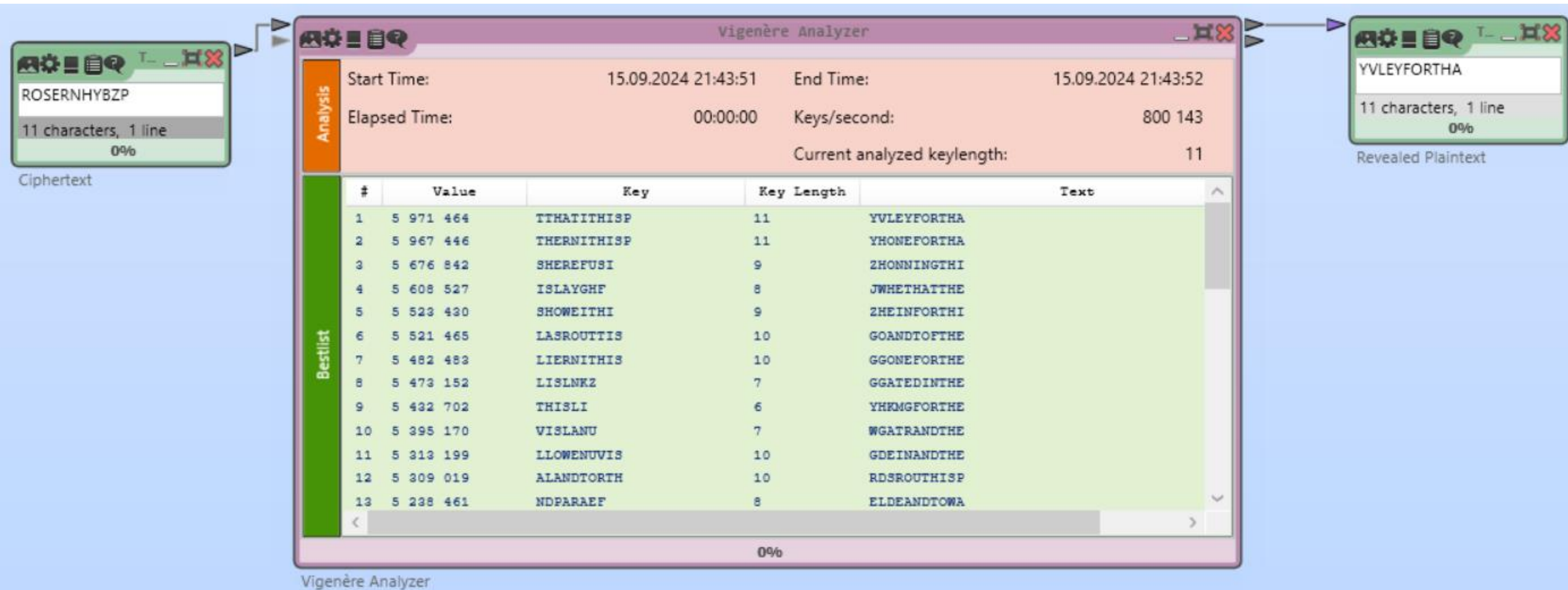
R	O	S	E	R	N	H	Y	B	Z	P				
P	H	O	N	E	P	H	O	N	E	P	H	O	N	E
C	H	E	R	N	Y	A	K	O	V	A				

CHERNYAKOVA

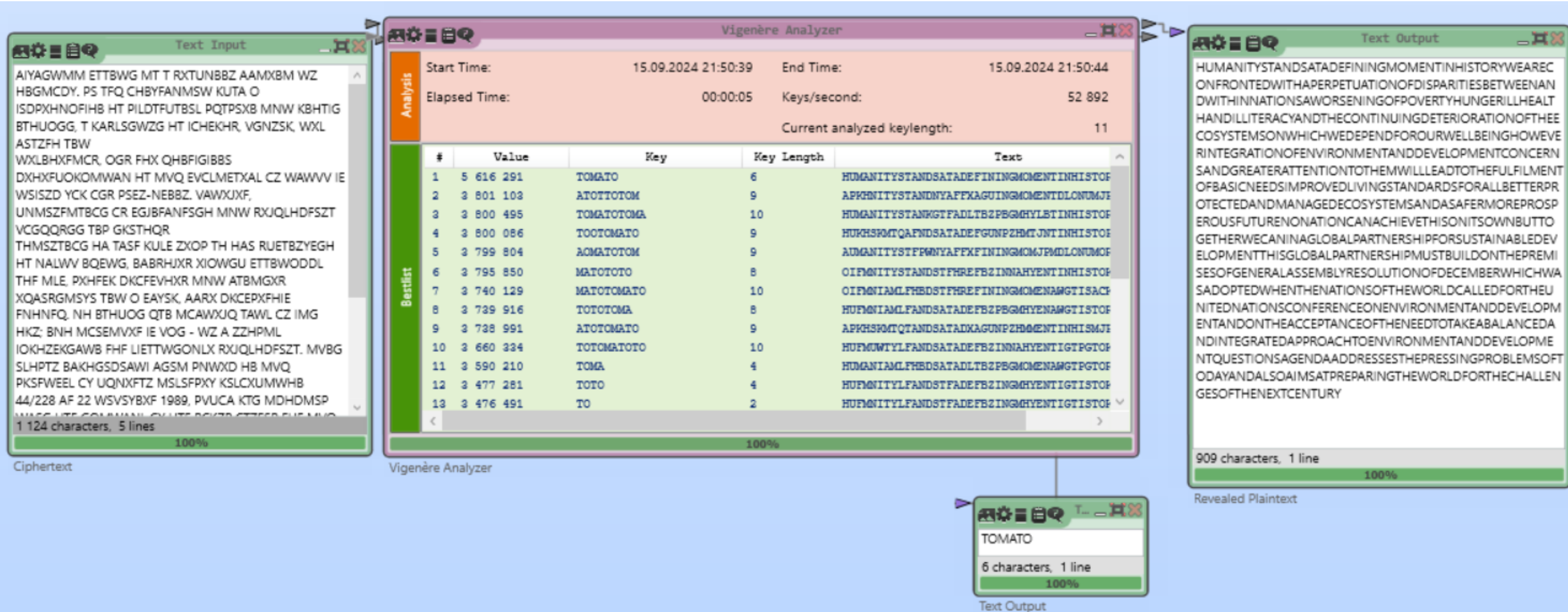
С применением CrypTool2



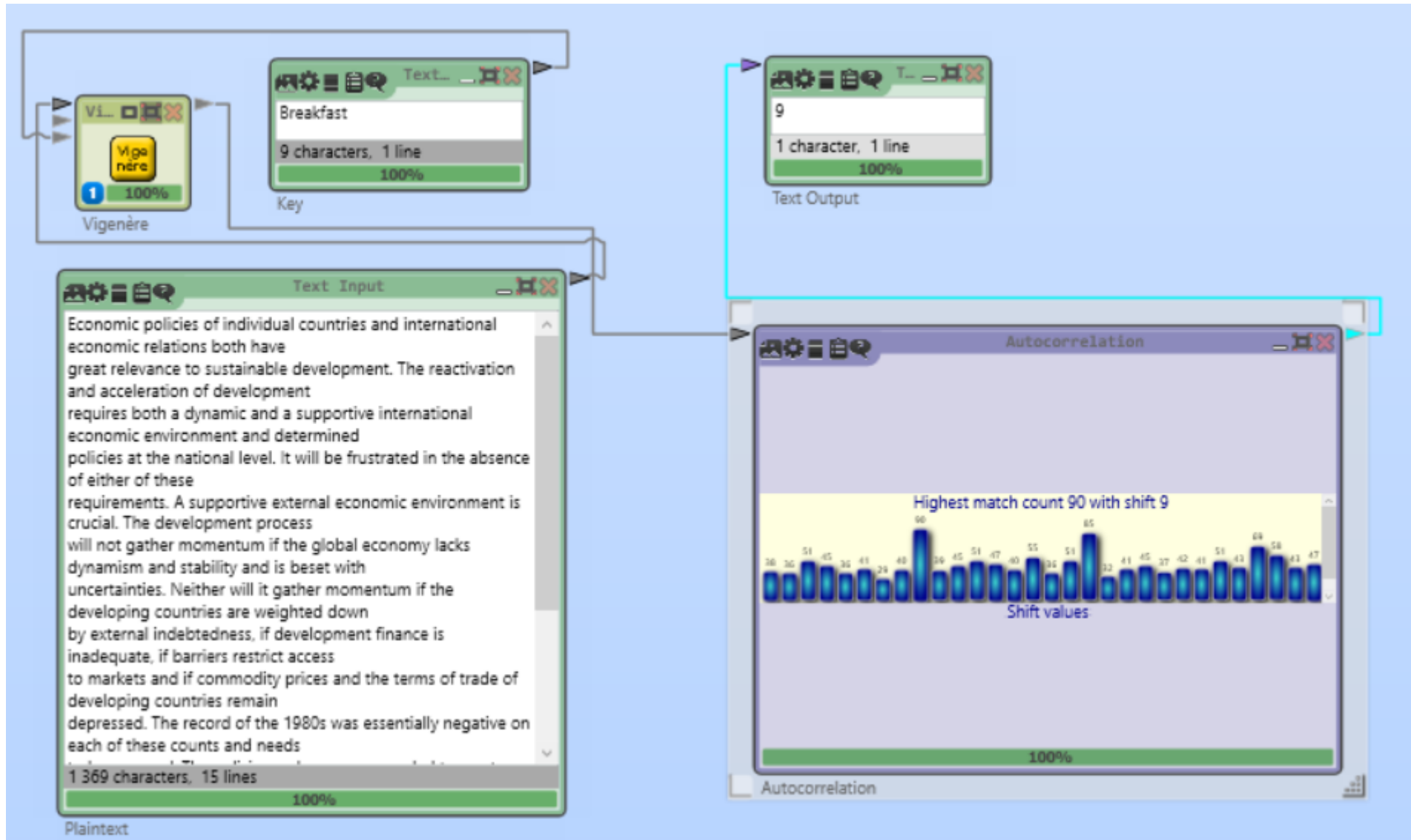
Атака на шифр



Атака на шифр (текст из файла English.txt)

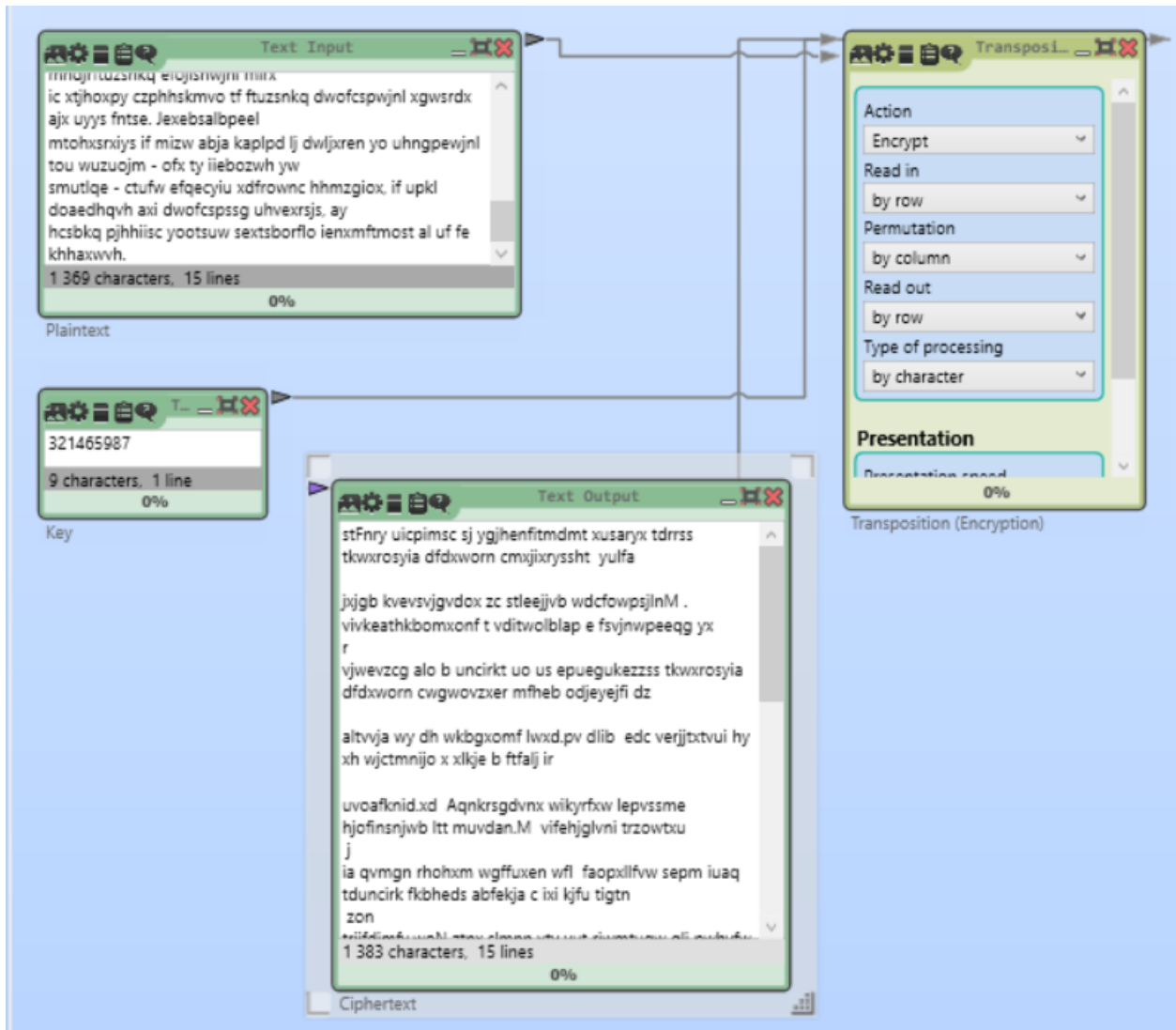


Атака на шифр в автоматизированном режиме



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:

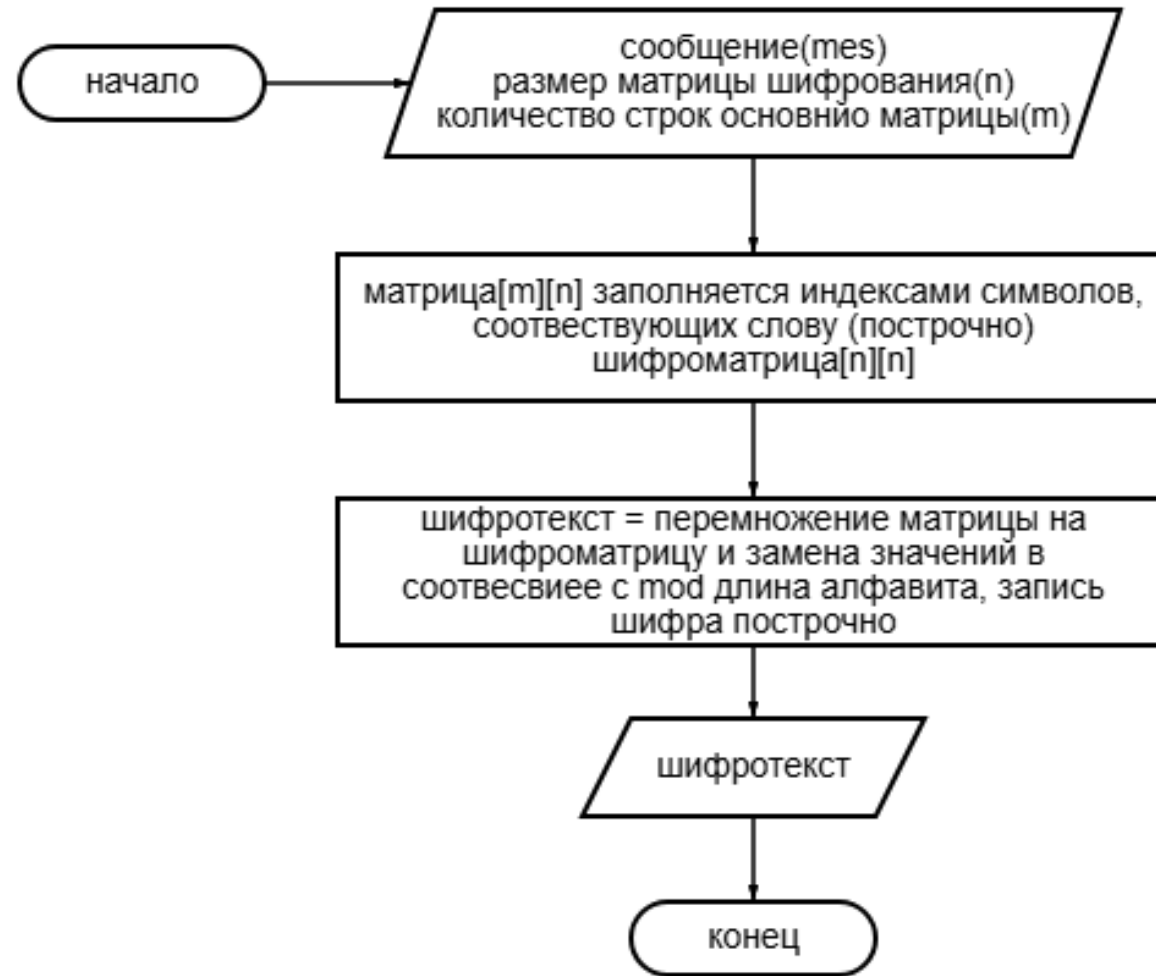
$O\left(\frac{n!}{(n-m)!}\right)$, где n и m – мощность алфавита и длина кодового слова соответственно.

Шифр Хилла (Hill)

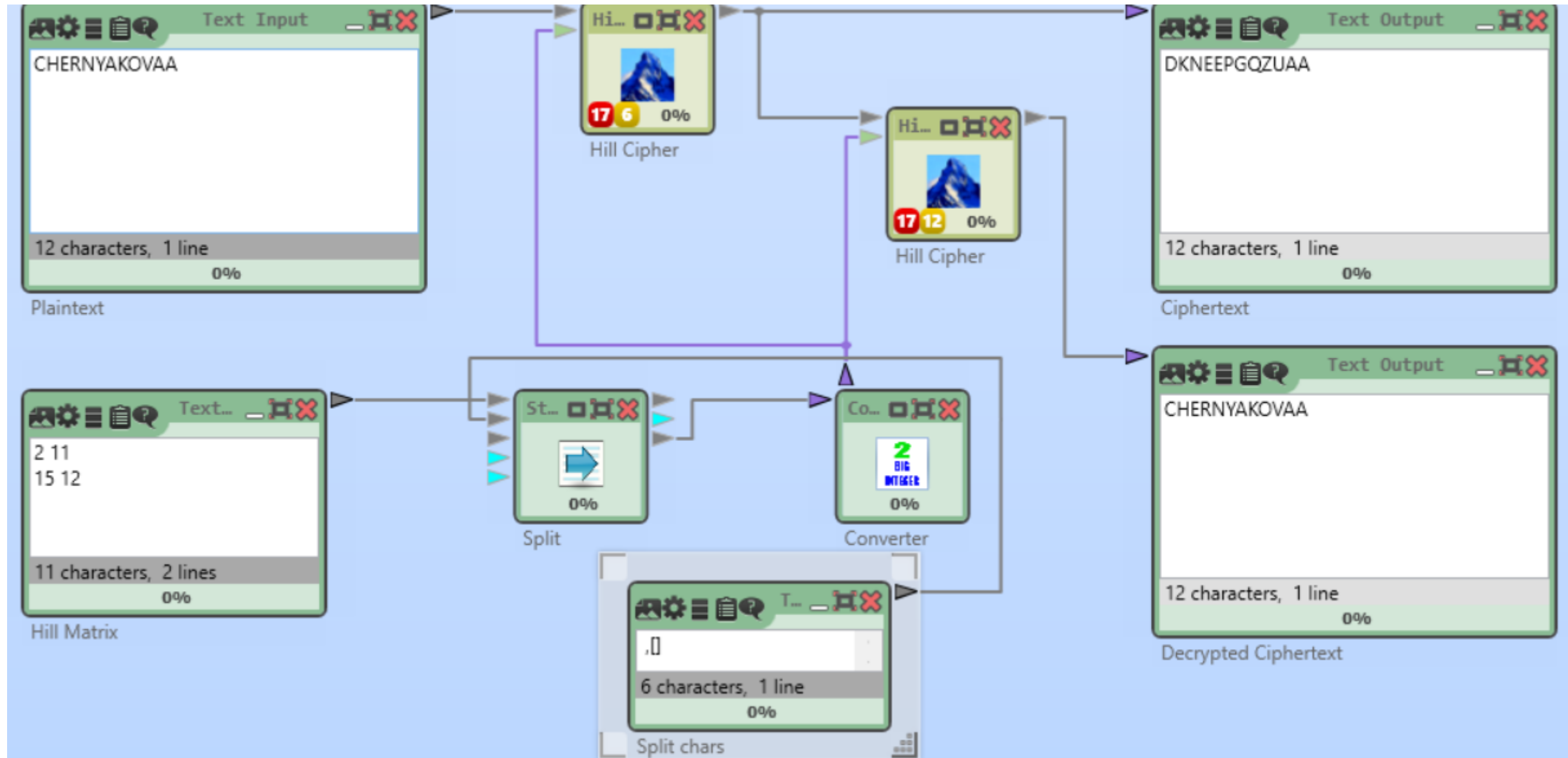
Задание

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 приложение 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

$$\begin{array}{|c|c|} \hline C & H \\ \hline E & R \\ \hline N & Y \\ \hline A & K \\ \hline O & V \\ \hline A & A \\ \hline \end{array} = \begin{array}{|c|c|} \hline 2 & 7 \\ \hline 4 & 17 \\ \hline 13 & 24 \\ \hline 0 & 10 \\ \hline 14 & 21 \\ \hline 0 & 0 \\ \hline \end{array} \times \begin{array}{|c|c|} \hline 2 & 15 \\ \hline 11 & 12 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 81 & 114 \\ \hline 195 & 264 \\ \hline 290 & 483 \\ \hline 110 & 120 \\ \hline 259 & 462 \\ \hline 0 & 0 \\ \hline \end{array} \pmod{26} = \begin{array}{|c|c|} \hline 3 & 10 \\ \hline 13 & 4 \\ \hline 4 & 15 \\ \hline 6 & 16 \\ \hline 25 & 20 \\ \hline 0 & 0 \\ \hline \end{array} = \text{DKNEEPGQZUAA}$$

$$\begin{array}{|c|c|} \hline D & K \\ \hline N & E \\ \hline E & P \\ \hline G & Q \\ \hline Z & U \\ \hline A & A \\ \hline \end{array} = \begin{array}{|c|c|} \hline 3 & 10 \\ \hline 13 & 4 \\ \hline 4 & 15 \\ \hline 6 & 16 \\ \hline 25 & 20 \\ \hline 0 & 0 \\ \hline \end{array} \times \begin{array}{|c|c|} \hline 6 & 25 \\ \hline 1 & 14 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 28 & 215 \\ \hline 82 & 381 \\ \hline 39 & 310 \\ \hline 52 & 374 \\ \hline 170 & 905 \\ \hline 0 & 0 \\ \hline \end{array} \pmod{26} = \begin{array}{|c|c|} \hline 2 & 7 \\ \hline 4 & 17 \\ \hline 13 & 24 \\ \hline 0 & 10 \\ \hline 14 & 21 \\ \hline 0 & 0 \\ \hline \end{array} = \text{CHERNYAKOVA}$$

Атака на шифр

Hill Analysis (Known Plaintext) ✕

This is a known-plaintext analysis of Hill encryption. If the plaintext is available along with the ciphertext, the Hill key can be recomputed.

Plaintext | Ciphertext

DEARIVANOVIVANOVICHTHANKYOU

Display Hill Key Matrix ✕

Selected alphabet (26 characters)

ABCDEFGHIJKLMNOPQRSTUVWXYZ Value of the first alphabet character 0

Hill key matrix

Alphabet characters	Number values
C N O	02 13 14
B B C	01 01 02
V C F	21 02 05

Text Output ✕

GHTQPKBPSYTQVDOQVMXZMXVVOHEIKQF
XOUNXIKROBKQAIDATYQANQTDUPVWNVN
ZJVDCYETFDRNUMSZOQXWJTVMOQWYRB
GQAIAFAOBKMLTLMWMWIOBKWEBHYPOH
WDIRWVPJWGTGXEVJAZVT

141 characters, 1 line

100%

Заключение

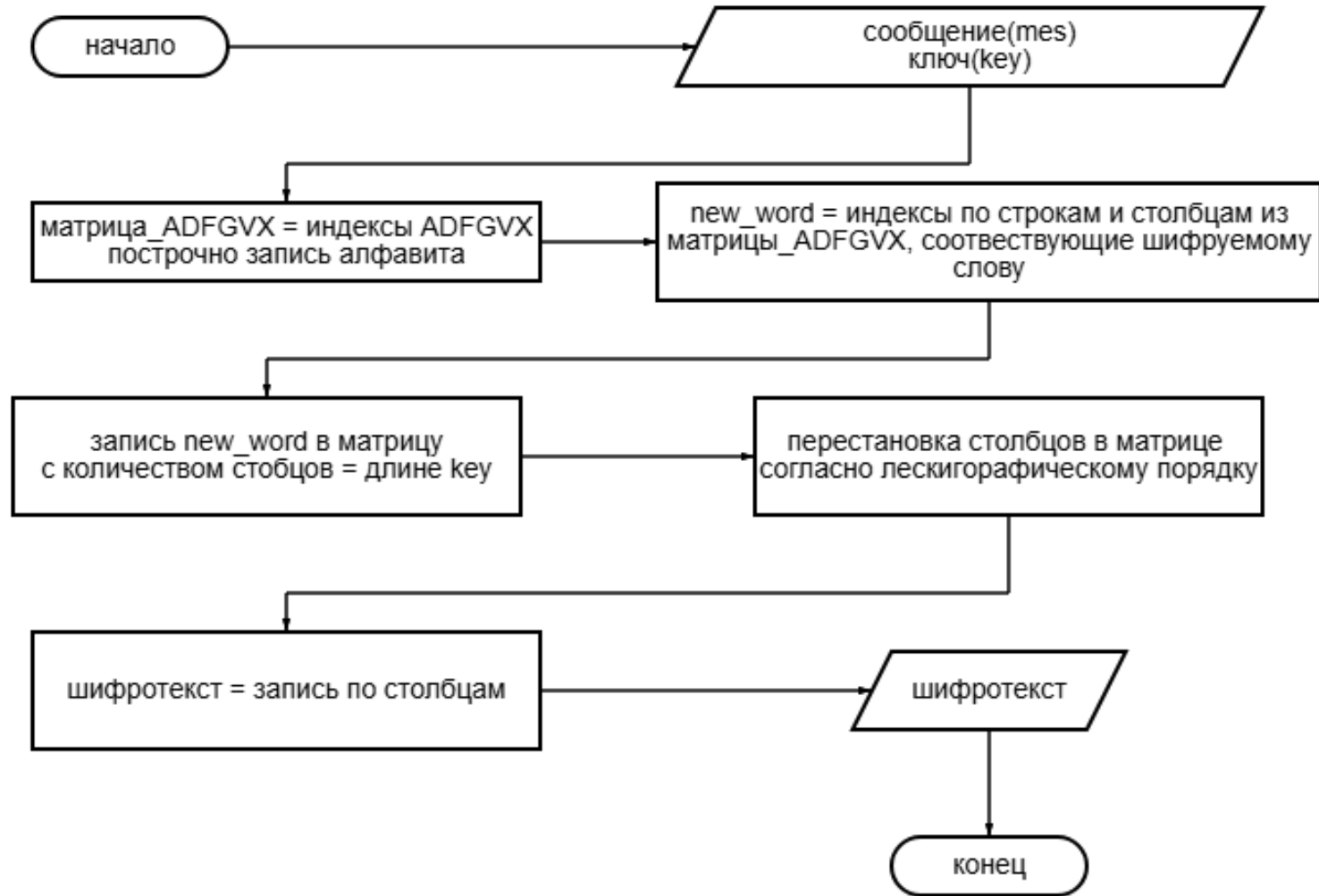
- Изучен шифр Хилла и выявлены его следующие основные характеристики:
 - Тип шифра – замена;
 - Ключ шифра – шифрующая матрица.
- Проведена атака методом грубой силы на шифр Хилла и выявлены ее следующие основные характеристики:
 - Оценка сложности атаки следующая:
 $O(n^{m \times m})$, где n и m – мощность 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

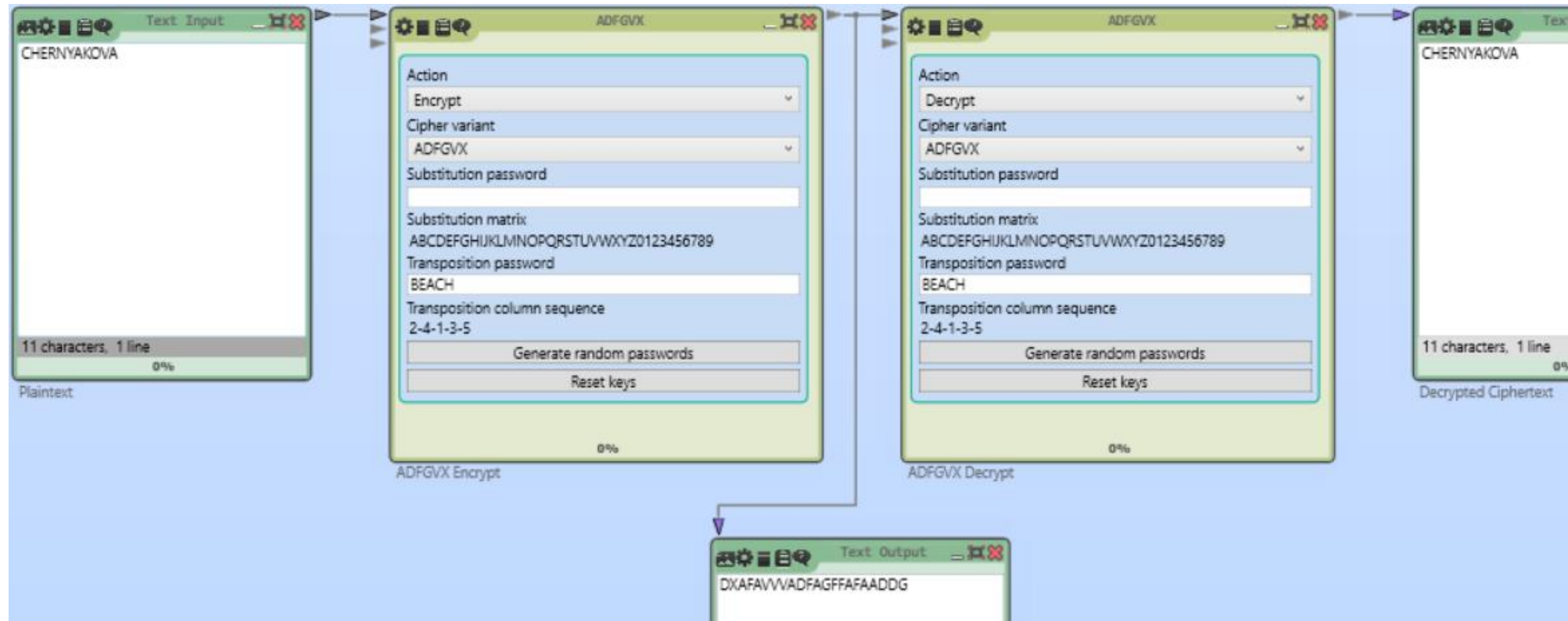
	A	D	F	G	V	X
A	A	B	C	D	E	F
D	G	H	I	J	K	L
F	M	N	O	P	Q	R
G	S	T	U	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

AFDDAVFXFDVAAADVFFGGAA

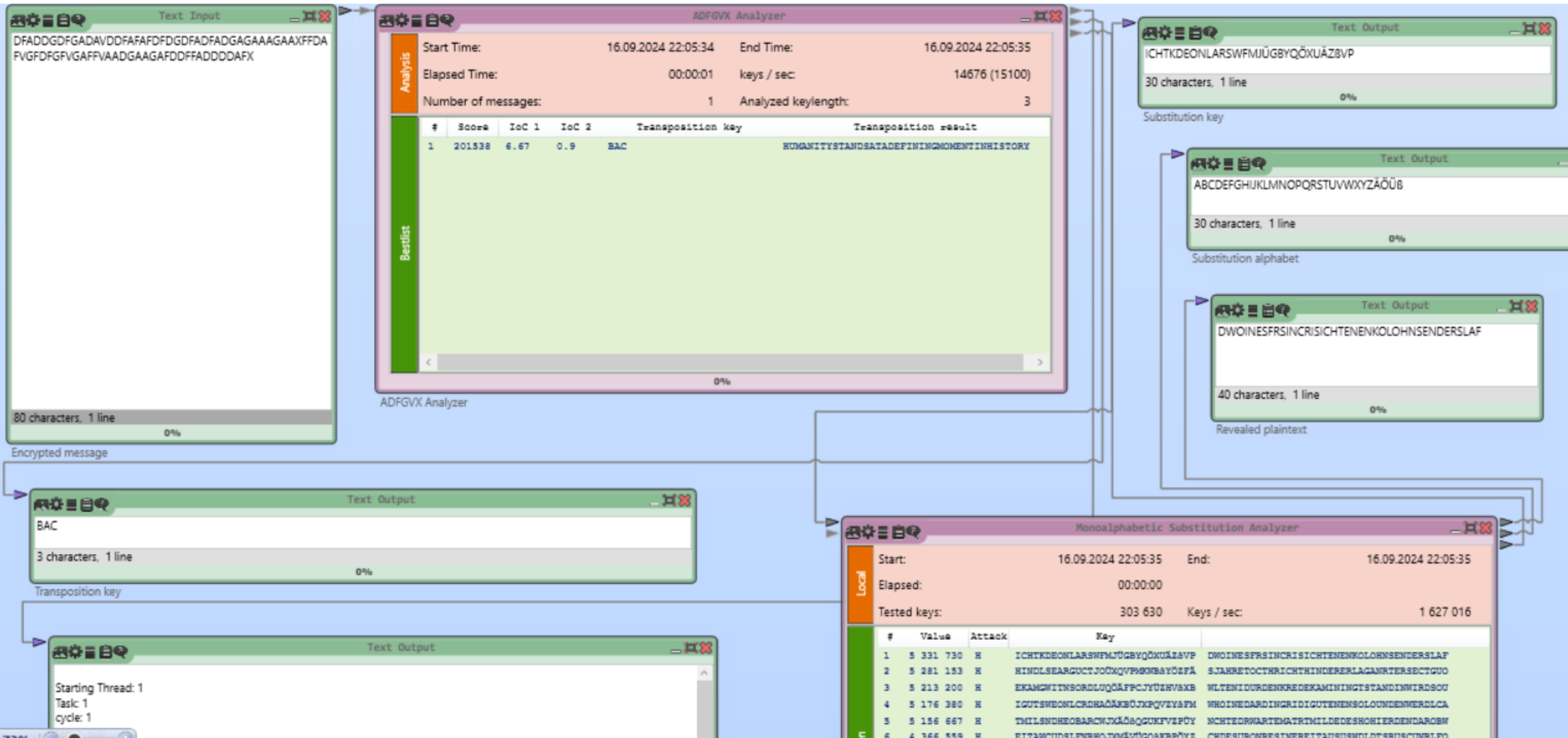
B	E	A	C	H
2	4	1	3	5
A	F	D	D	A
V	F	X	F	D
V	A	A	A	D
V	F	F	G	G
A	A			

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	

DXAFVAVVADVFAGFFAFAADDG



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.