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

Лабораторная работа № 1, 2, 3

Изучение классических шифров Stytale, Caesar, Substitution, Permutation/Transposition, Vigenere, Hill, Adfgvx

Студент Усачева Дарья Владимировна, гр. 1384

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

Санкт-Петербург, 2024

Цель работы

Исследовать шифры Stytale, Caesar, Substitution, Permutation/Transposition, Vigenere, Hill, ADFVGX. Получить практические навыки работы ними, в том числе с использованием приложения Cryptool 1, 2. Повысить свою компетенцию в области классических шифров и в криптографии в целом.

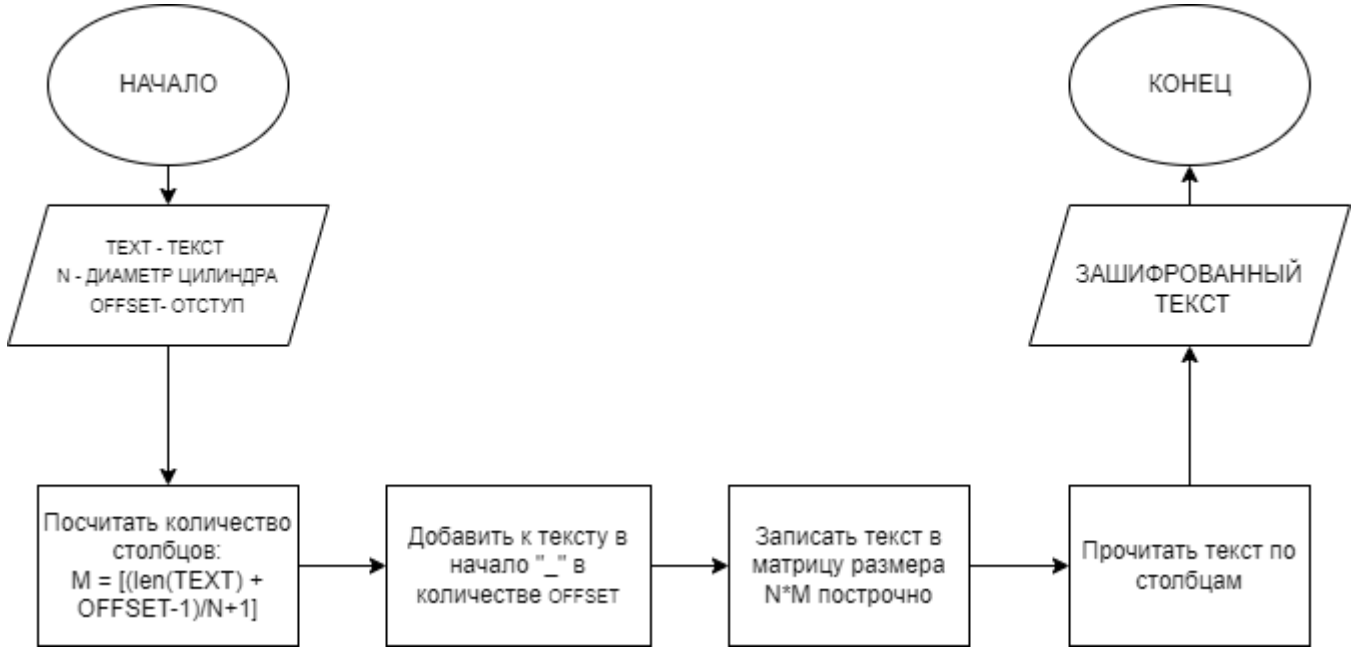
Шифр Scytale

Задание

1. Найти шифр в CrypTool 1: Encrypt/Decrypt –> Symmetric(Classic) Scytal/Rail Fence.
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.

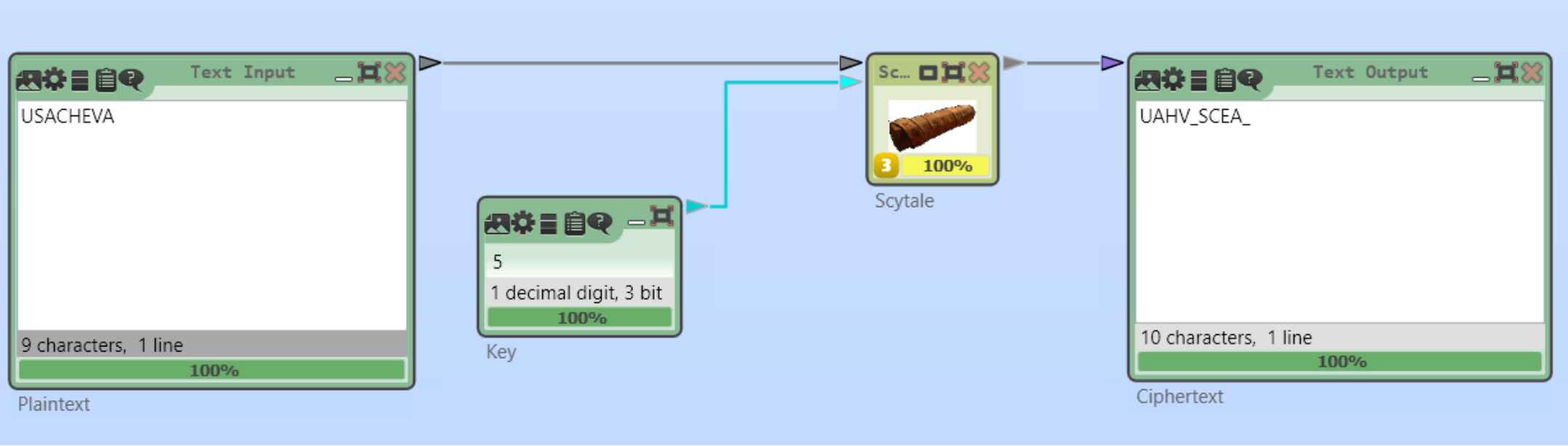
Изучить принципы этой автоматической атаки

Схема алгоритма зашифрования сообщения

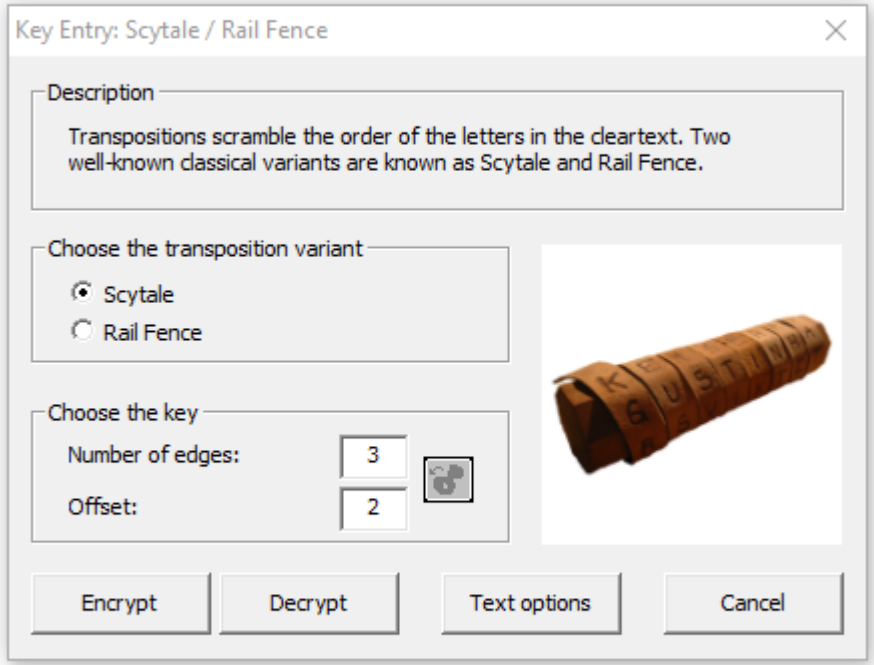


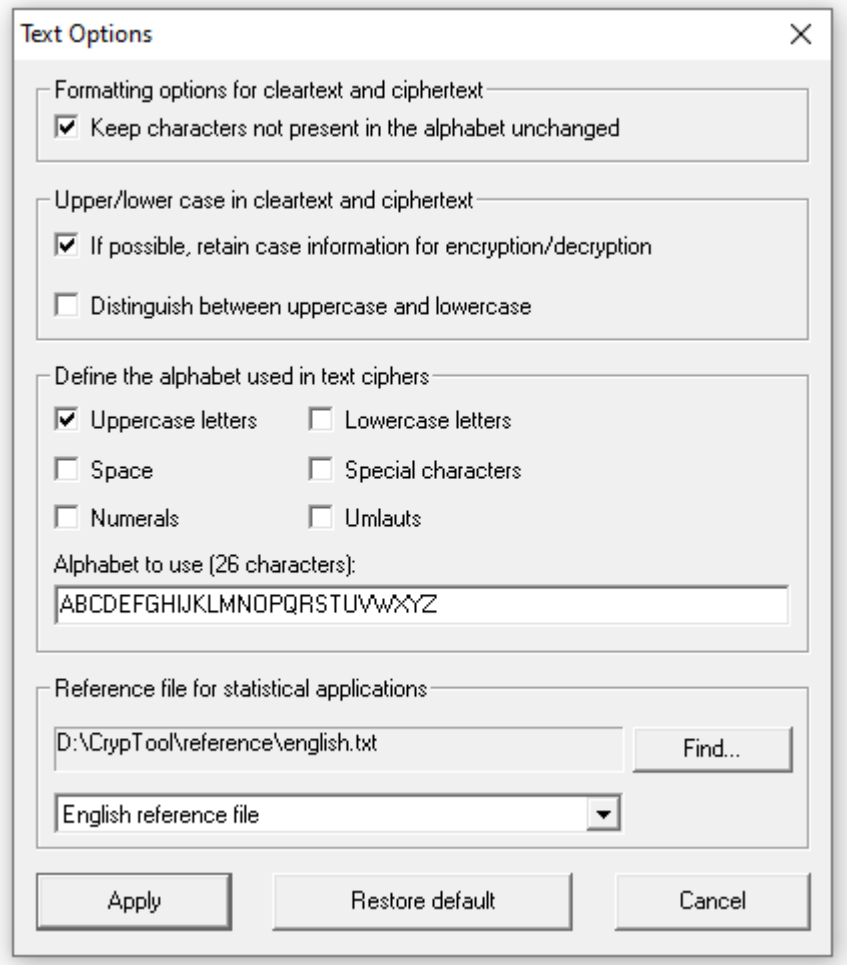
Визуальная схема

Так как в Cryp Tool 2 отсутствует функционал для изменения параметра Offset для алгоритма Scytale, поэтому задание выполнялось в Cryp Tool 1, а схема была нарисована в Cryp Tool 2

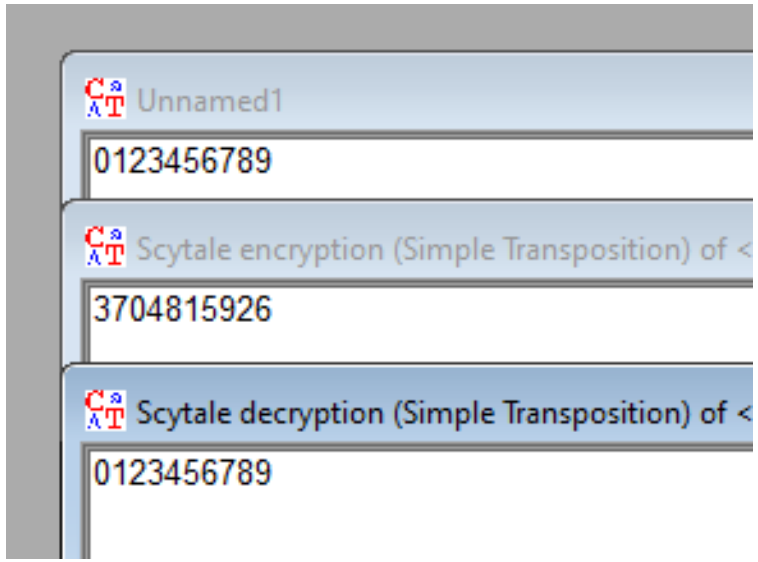


Реализация в CrypTool 1



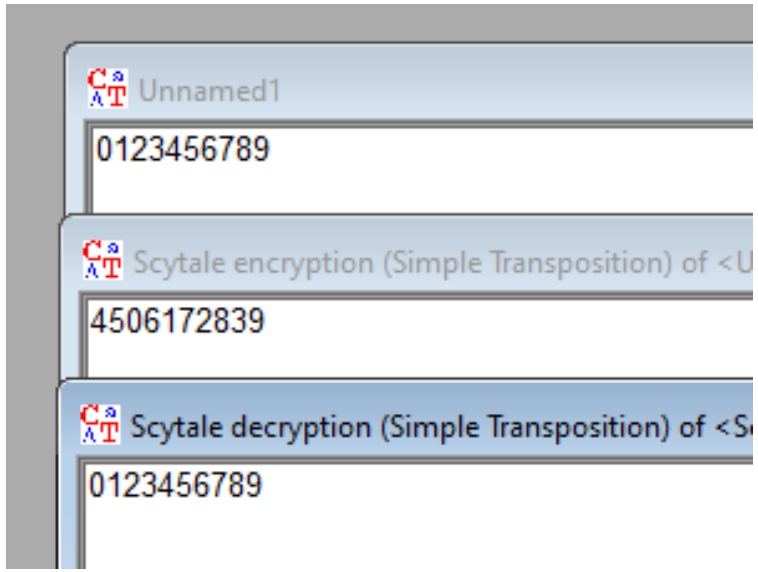


Задание 1-3



Number of Edges = 3

Offset = 1



Number of Edges = 2

Offset = 2

Задание 4

В результате запуска было установлено как параметры Number of Edges и Offset влияют на шифрование:

- Numbers of edges — число граней цилиндра, что говорит о числе строк матрицы, в которую записывается слово. (Число столбцов считается как (длина текста + offset) / numbers of edges)
- Offset — число пустых клеток в начале матрицы, в которые не надо писать буквы.

Задание 5

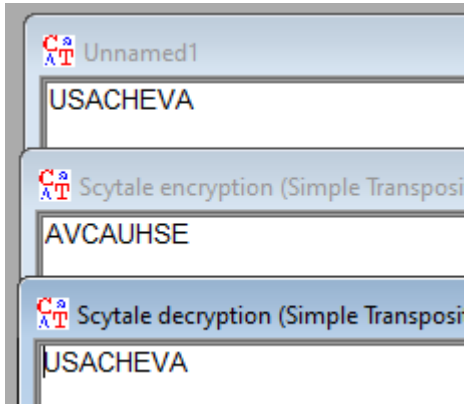
Были выбраны параметры:

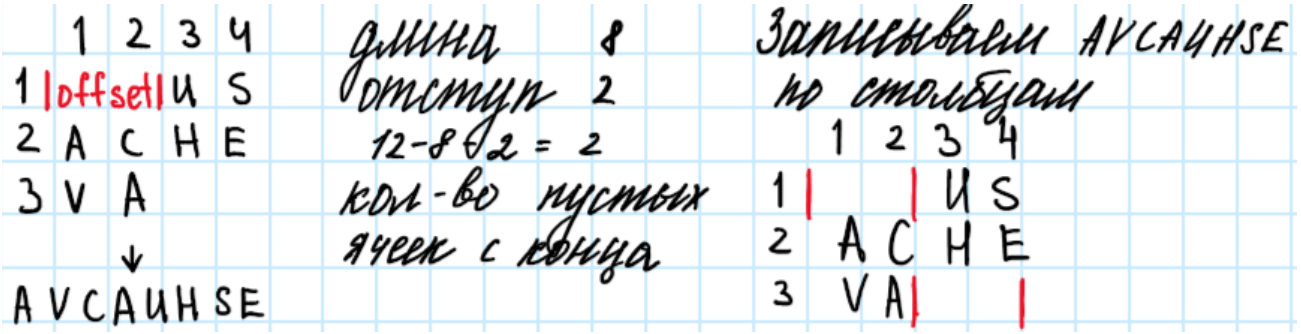
Number of Edges = 3

Offset = 2

Текст был зашифрован и расшифрован вручную и с помощью CrypTool 1.

Результаты совпадают.

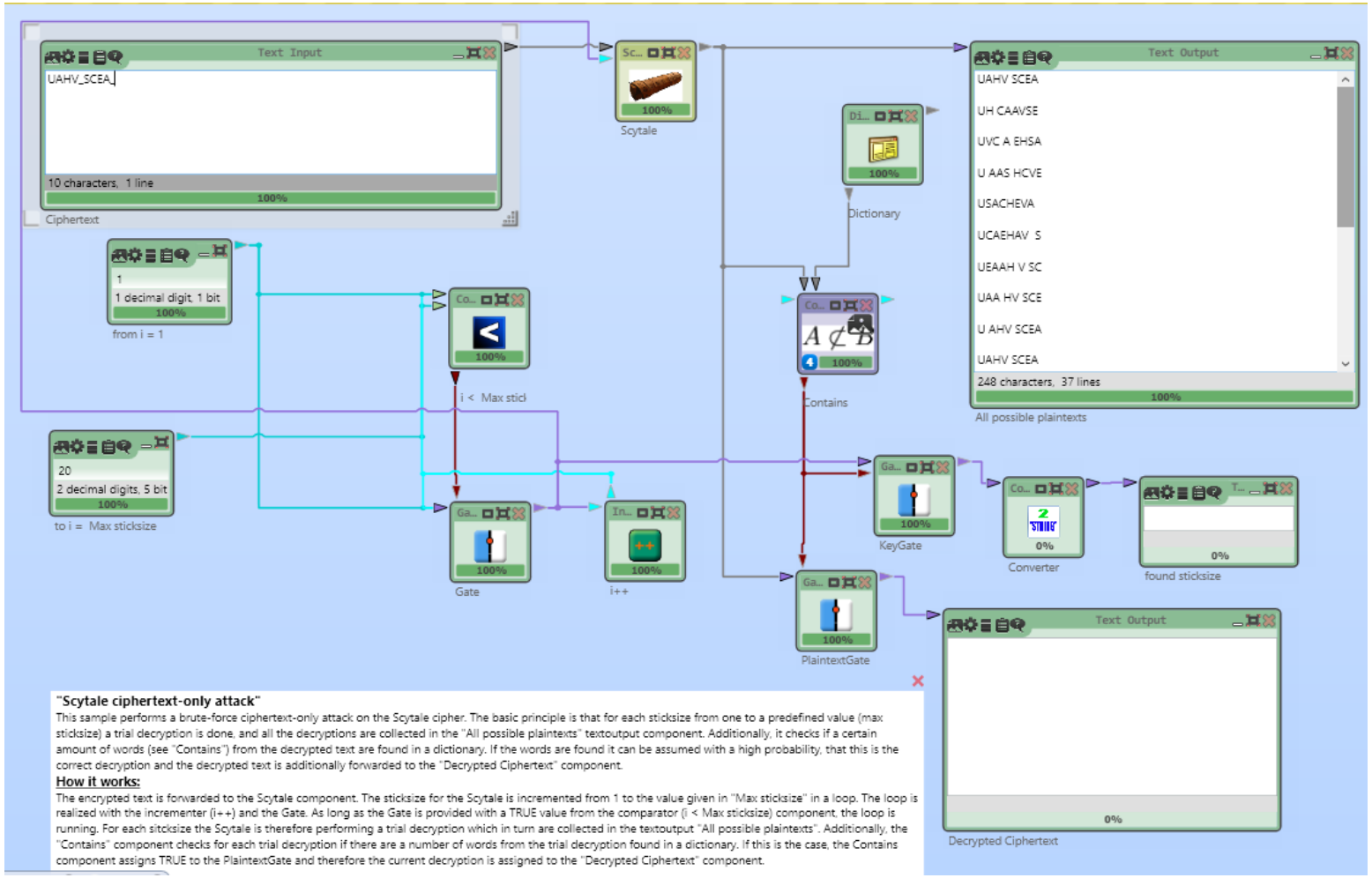




Задание 6

Была проведена атака методом «грубой силы» на зашифрованный текст. Был введен текст, полученный с помощью шифрования USACHEVA -> UAHV_SCEA_ (Number of Edges = 5 Offset =0)

Правильный результат был получен с 5 попытки дешифрования



Основные характеристики шифра

Тип шифра: перестановочный.

Ключ: количество граней на цилиндре.

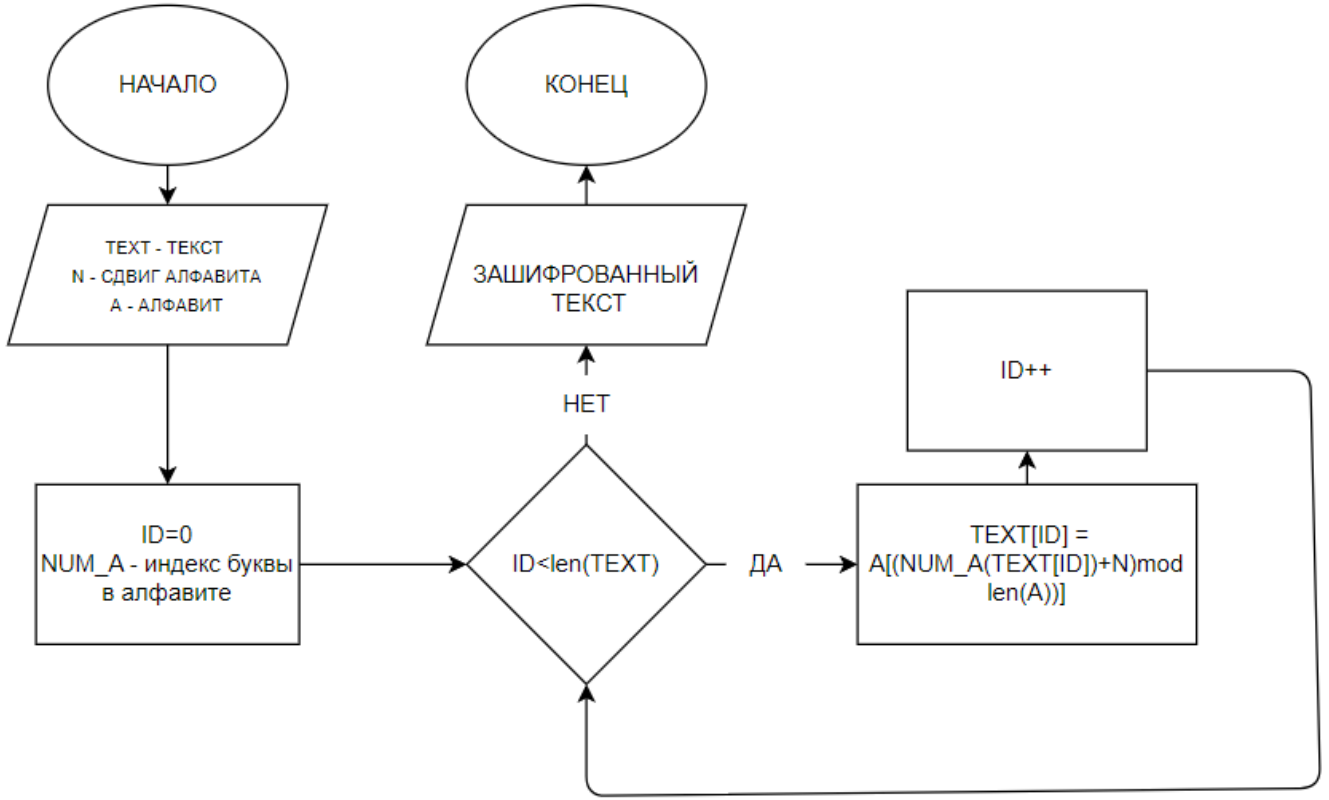
Если граней всего одна или текст слишком короткий, то шифровать нет смысла.
В обычном случае асимптотическая сложность составляет O(n), где n – длина текста. А если использовать смещение (от 0 до n), то асимптотическая сложность возрастает до $O(n^2)$.

Шифр Caesar

Задание

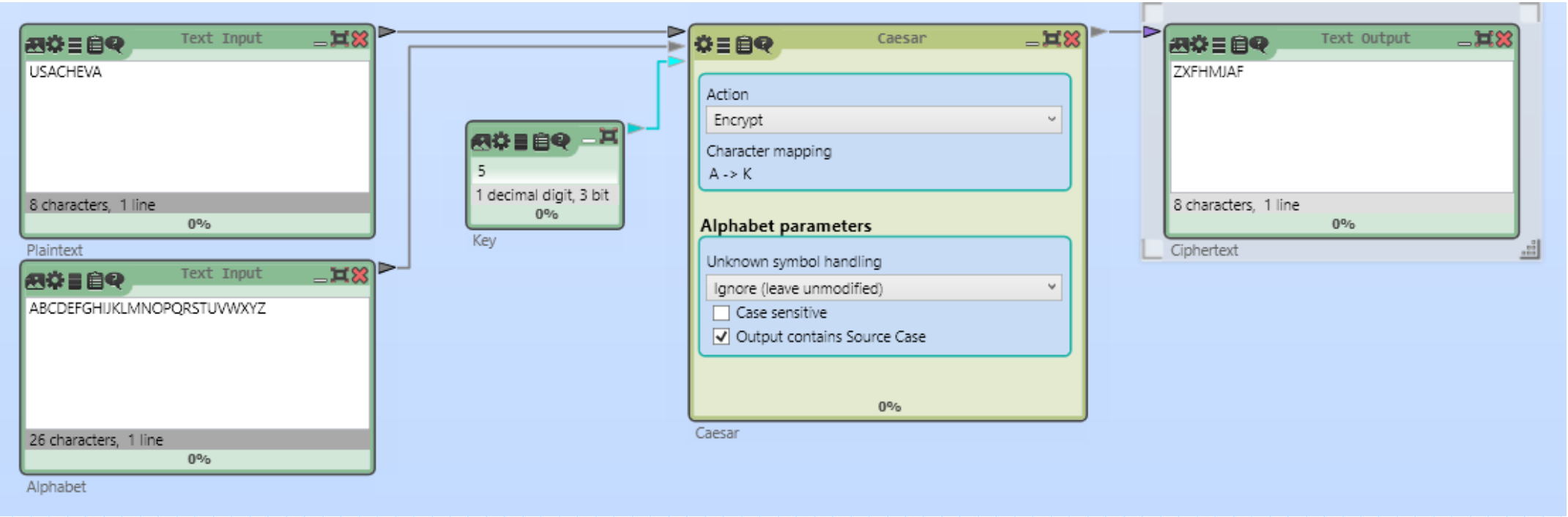
1. Найти шифр в CrypTool 1: Encrypt/Decrypt –> Symmetric(Classic) –> Caesar/Rot-13.
2. Зашифровать и расшифровать текст, содержащий только фамилию (транслитерация латиницей), вручную и с помощью шифра с ключом, отличным от 0. Убедиться в совпадении результатов.
3. Построить гистограмму частот букв английского языка по эталонному файлу English.txt (папка CrypTool/reference), используя утилиту из Analysis –> Tools for Analysis.
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.
7. Выполнить самостоятельную работу: обменяться шифровками с коллегой по группе для проведения подобной атаке по дешифрации сообщения.

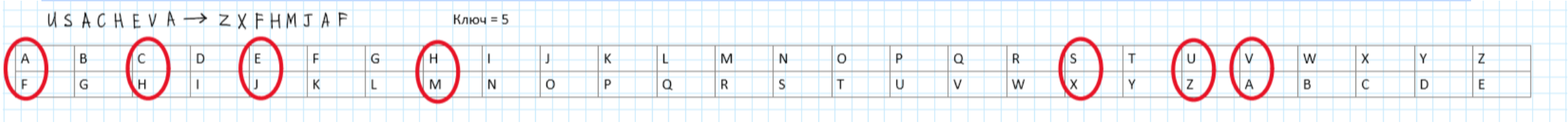
Схема алгоритма зашифрования сообщения



Задание 1-2

Текст был зашифрован и расшифрован вручную и с помощью CrypTool 2. Результаты совпадают.





Задание 3-5

Была построена гистограмма частот букв английского языка по эталонному файлу English.txt

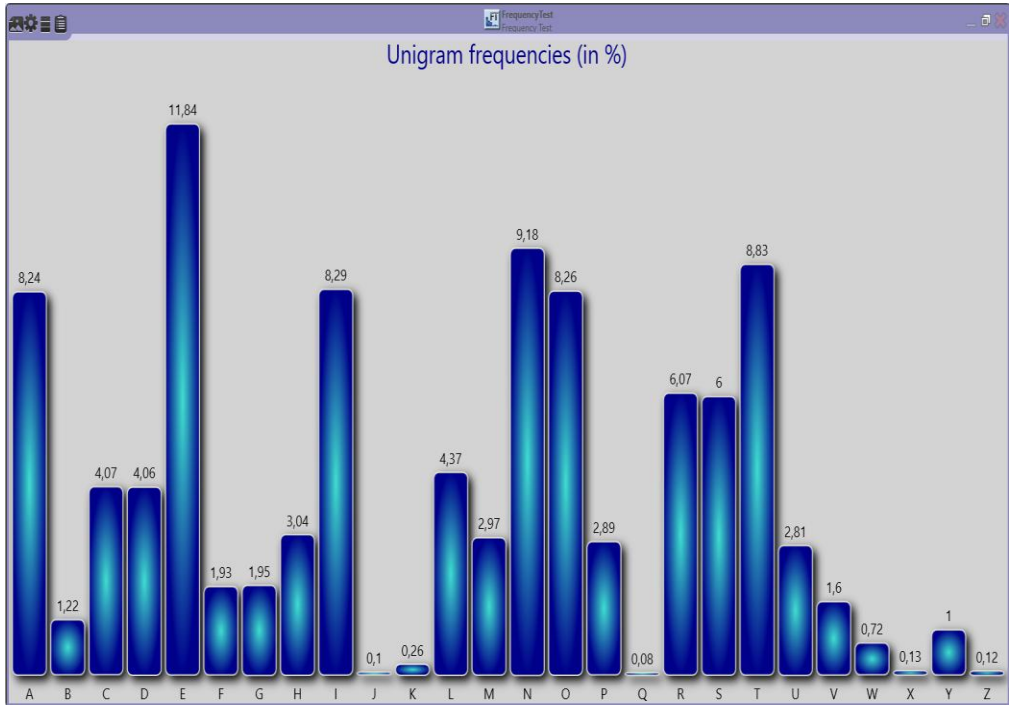
Был зашифрован текст из файла CrypTool-en.txt с ключом 5, затем была построена гистограмма частот для подтверждения ключа шифрования.

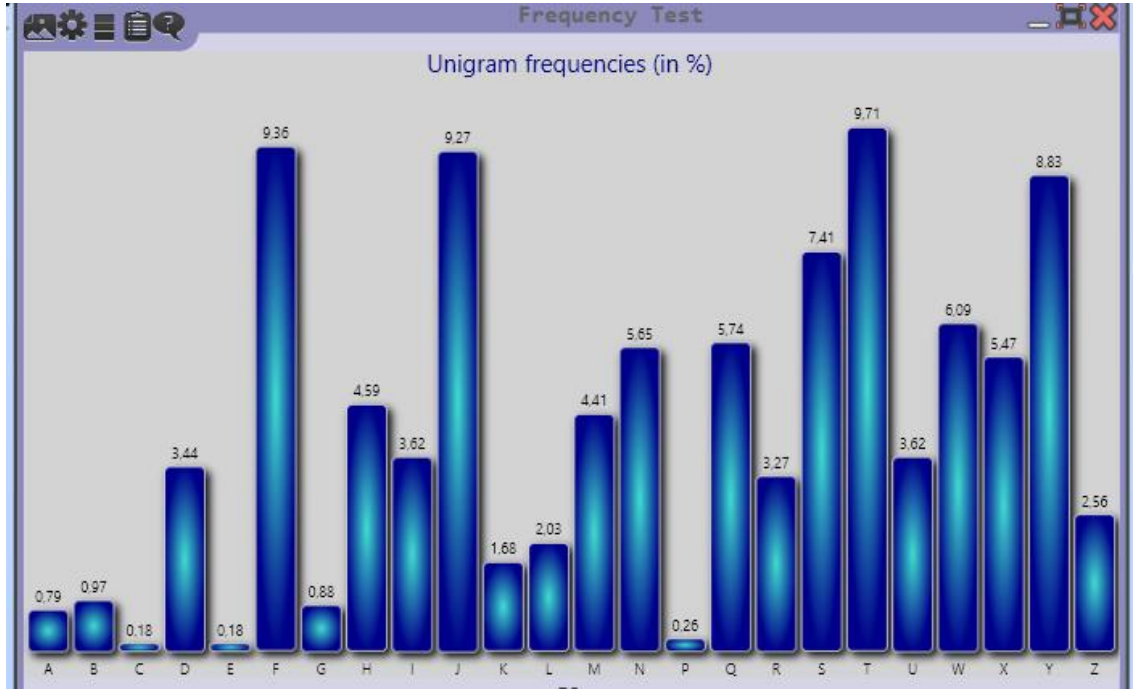
Сравним самые популярные буквы

В незашифрованном тексте : A, E, I, N, O, T.

В зашифрованном тексте : F, J, S, T, Y.

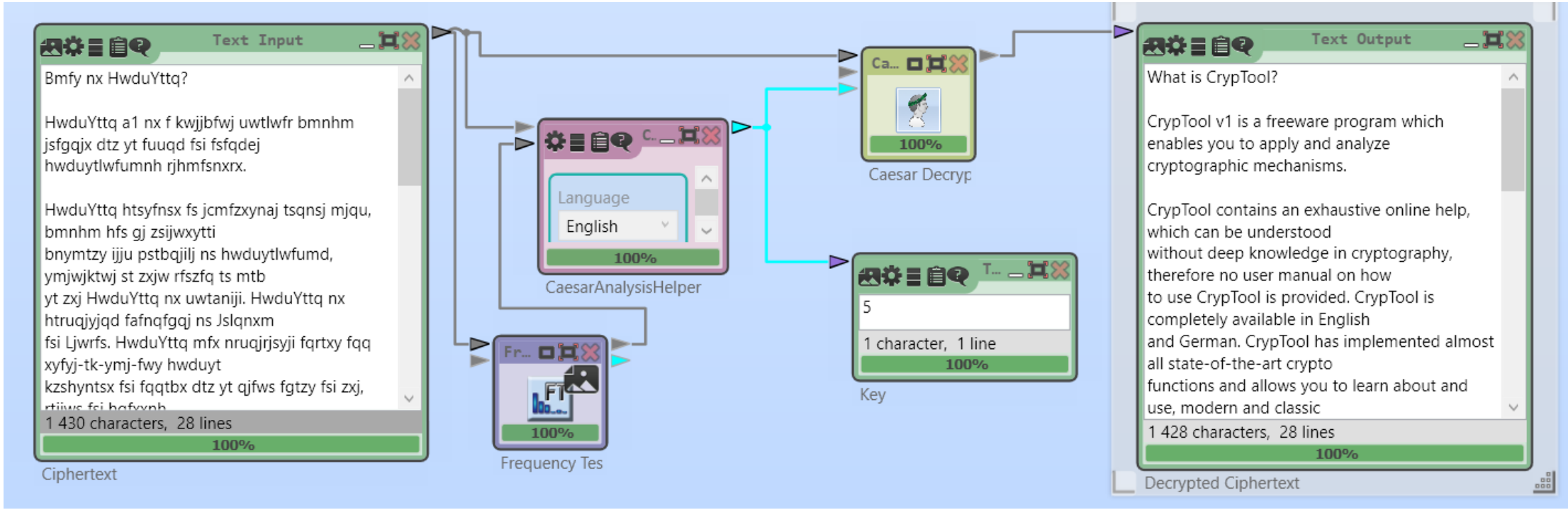
Это совпадает с результатом незашифрованного текста со смещением 5.





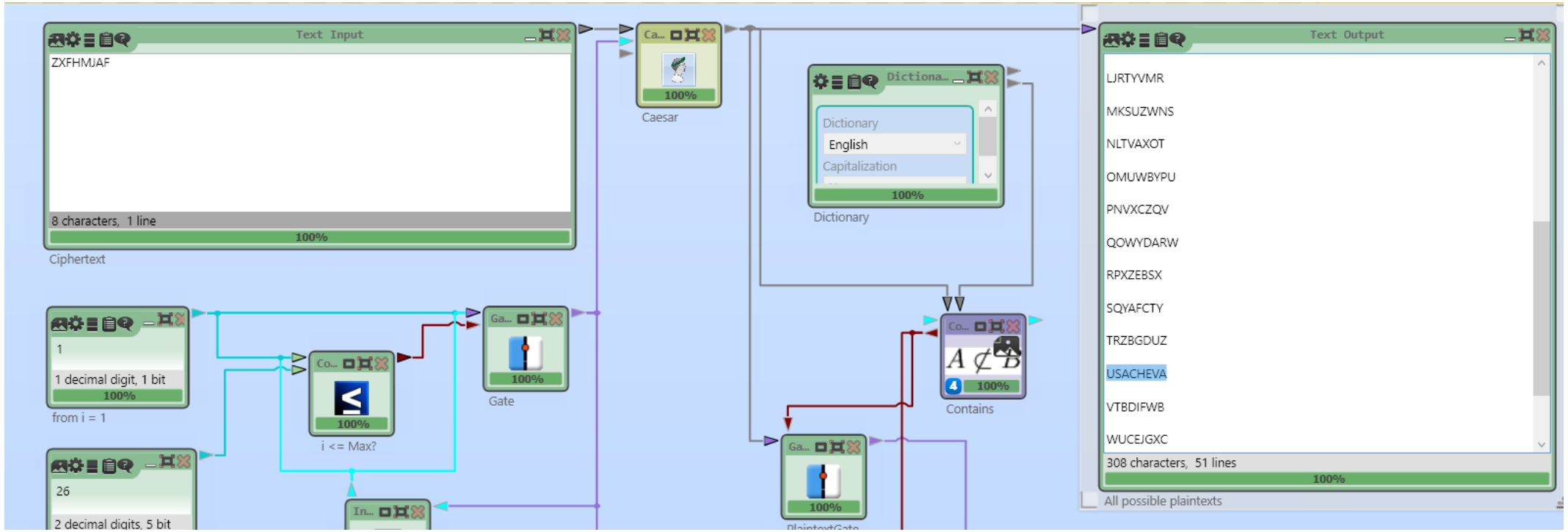
Задание 6

Была проверена гипотеза о значении ключа. Гипотеза оказалась верна, ключ равен 5.



Атака методом «грубой силы»

Была проведена атака методом «грубой силы» на зашифрованный текст. Как итог, был получен правильный результат.



Основные характеристики шифра

Тип шифра: замена.

Ключ: сдвиг алфавита.

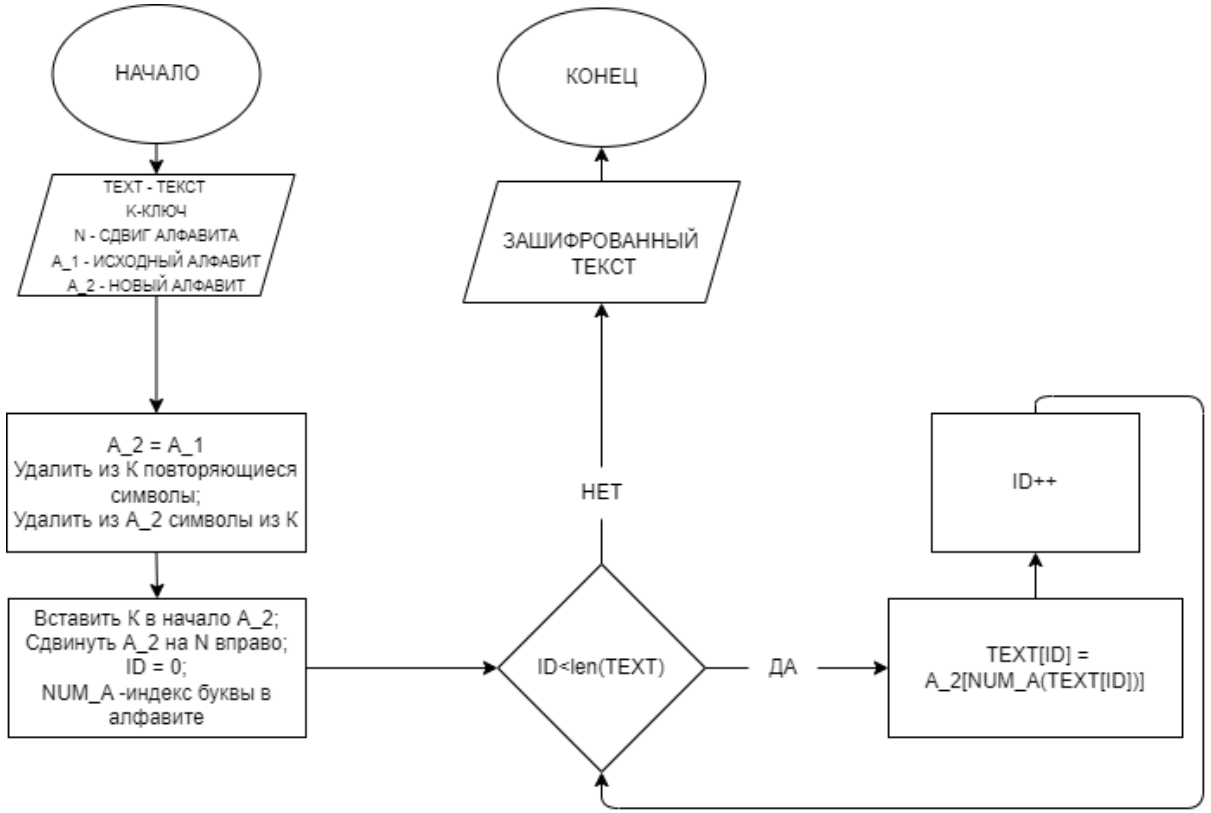
Сложность атаки “грубой силы” составляет O(n), где n - мощность алфавита

Шифр Substitution

Задание

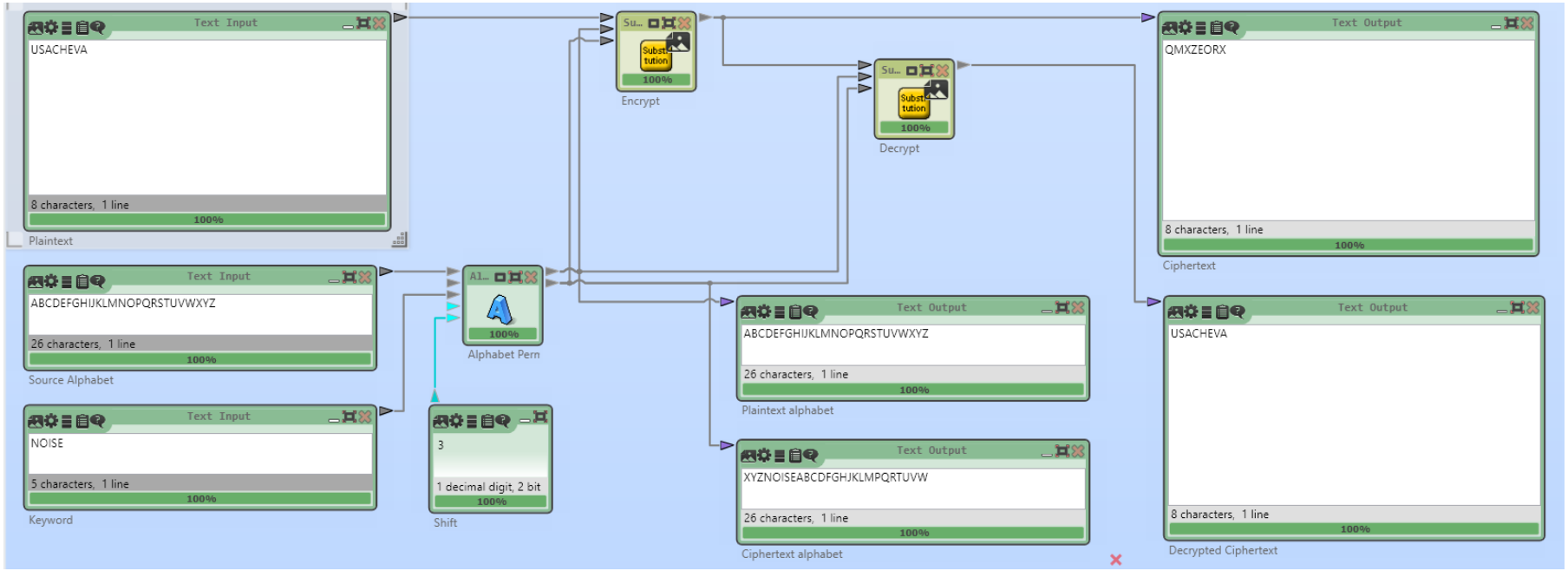
1. Найти шифр в CrypTool 1: Encrypt/Decrypt –> Symmetric(Classic).
2. Зашифровать и расшифровать текст, содержащий только вашу фамилию (транслитерация латиницей), вручную и с помощью шифра с выбранным ключом и смещением Offset ≠ 0. Убедиться в совпадении результатов.
3. Выполнить зашифрование и расшифрование 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.
10. Выполнить самостоятельную работу: а) зашифровать текст из 200 символов, сохранить ключ и обменяться шифровками с коллегой по учебной группе для дешифровки; б) изучить одну из атак, реализованных в CrypTool 1 и 2, опираясь на Help и ссылки на статьи.

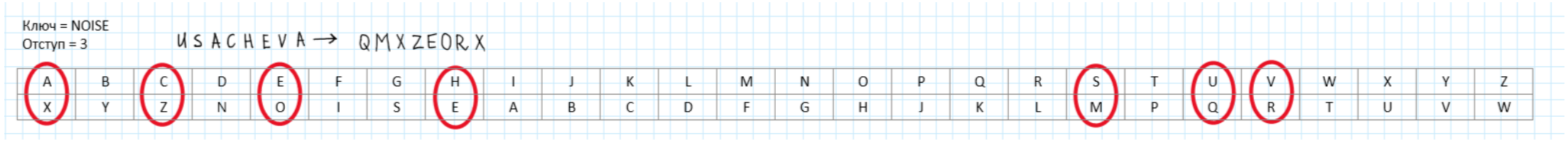
Схема алгоритма зашифрования сообщения



Задание 1-2

Текст был зашифрован и расшифрован вручную и с помощью CrypTool 2. Результаты совпадают.





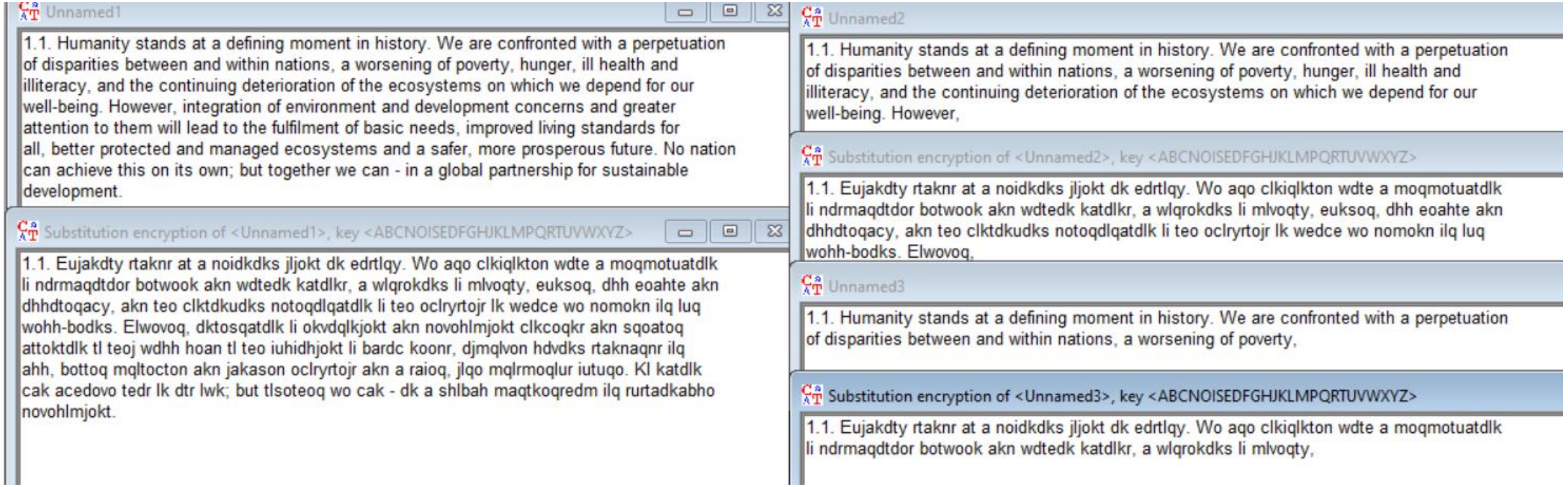
Задание 3

После выполнения зашифрования и расшифрования с различными паролями и смещениями было установлено, как формируется алфавит шифротекста:

1. Из ключевого слова удаляются дубликаты букв;
2. Полученная последовательность вставляется в начало алфавита (без этих букв);
3. Алфавит сдвигается вправо на количество букв равное смещению.

Задание 4-6

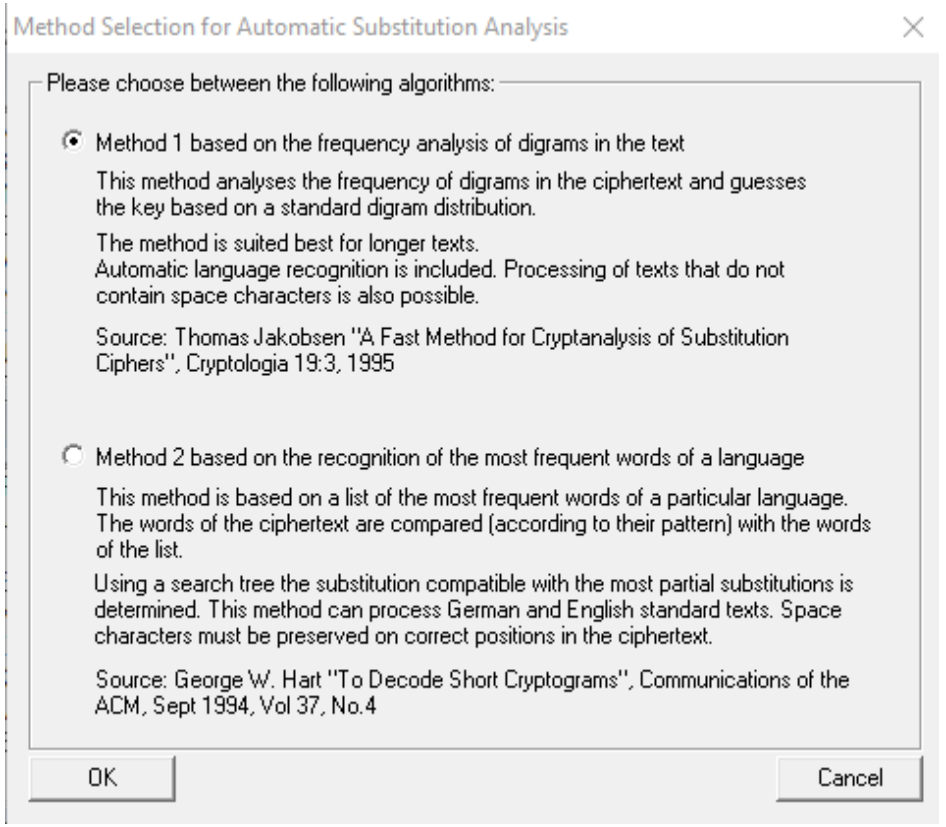
Взяты и зашифрованы 3 абзаца по 600, 300, 150.



Методы атаки на шифр в CrypTool 1.

Первый метод определяет частотное распределение данного текста. Подсчитывается частота появления каждой буквы шифротекста. Полученное распределение частот сравнивается, например, со справочной таблицей частот для символов языка открытого текста. Выдвигаются гипотезы о соответствии букв открытого текста и шифротекста. Сделанные гипотезы проверяются с помощью справочных таблиц распределения биграмм и триграмм.

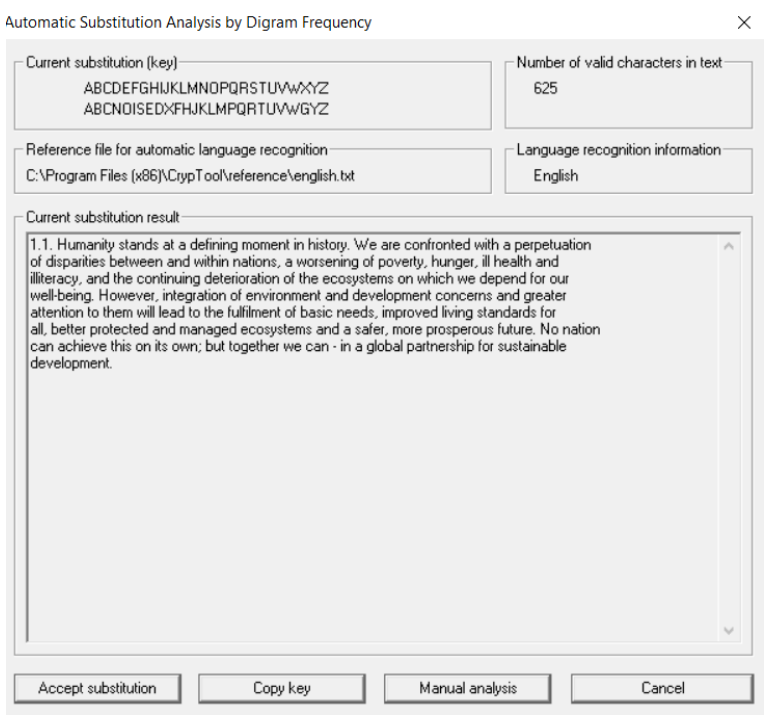
Второй метод пытается сопоставить наиболее часто встречающиеся слова языка со словами в данном зашифрованном тексте. Обязательным условием для применения метода является сохранение пробелов.

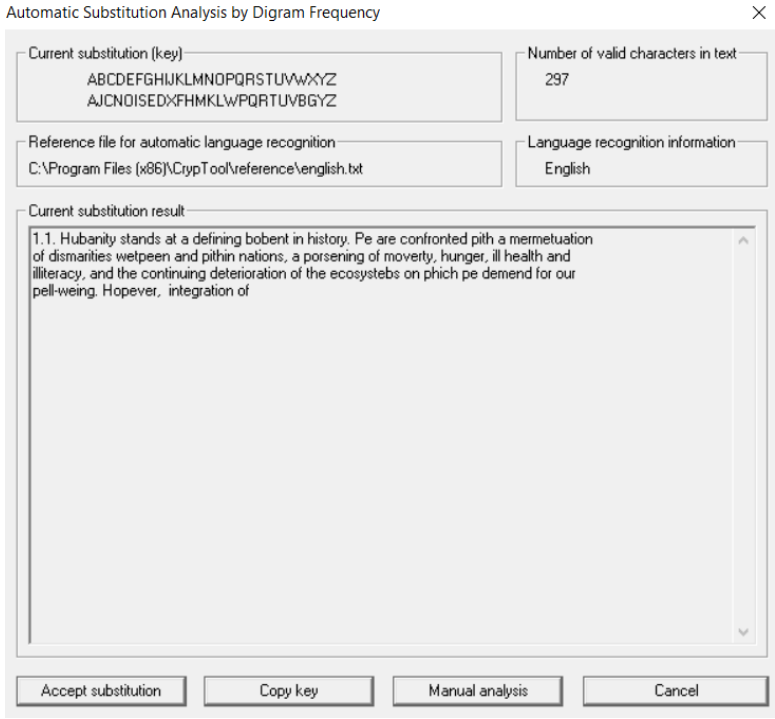


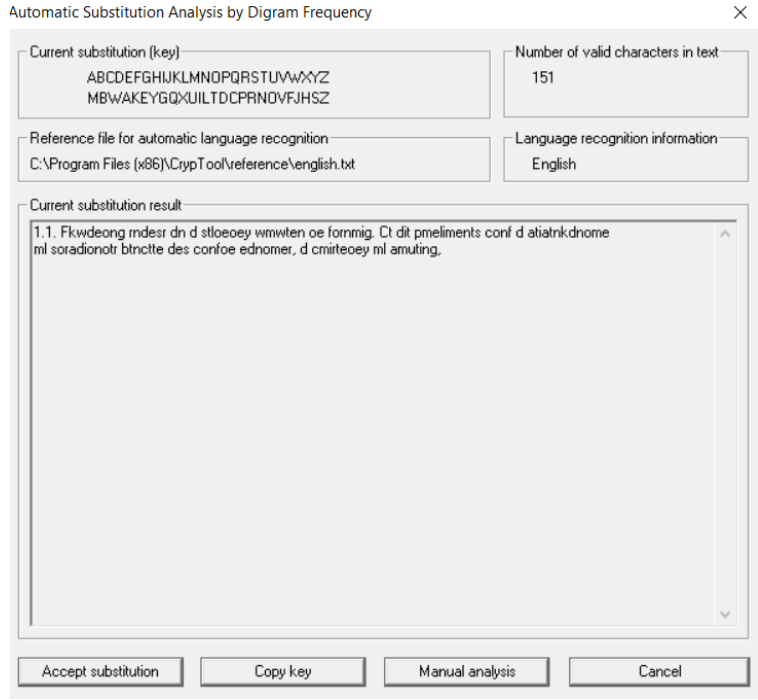
Задание 4-6

Выполнены атаки на шифротекст.

Как можно заметить, исходный текст совпадает с результатом атаки для 600 символов. Для 300 символов текст расшифрован частично верно. Для 150 символов текст расшифрован неверно, так как он слишком короткий.





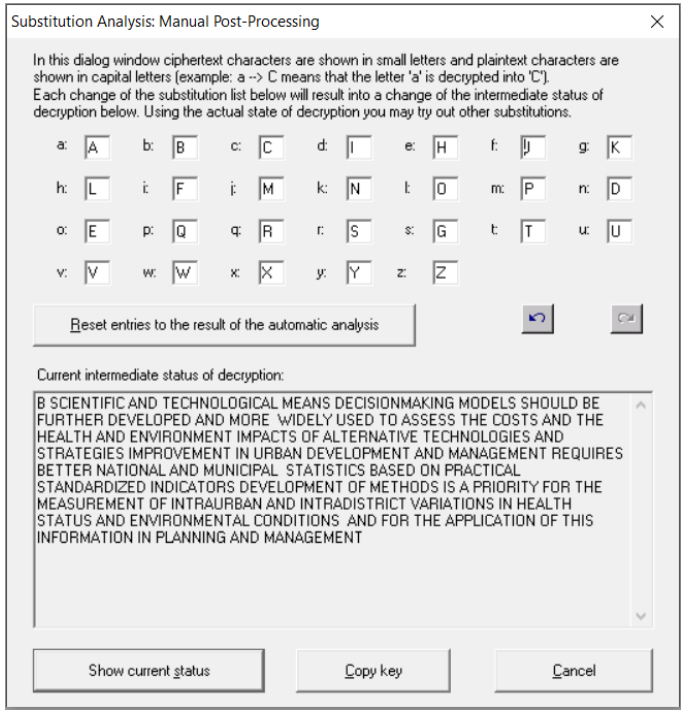


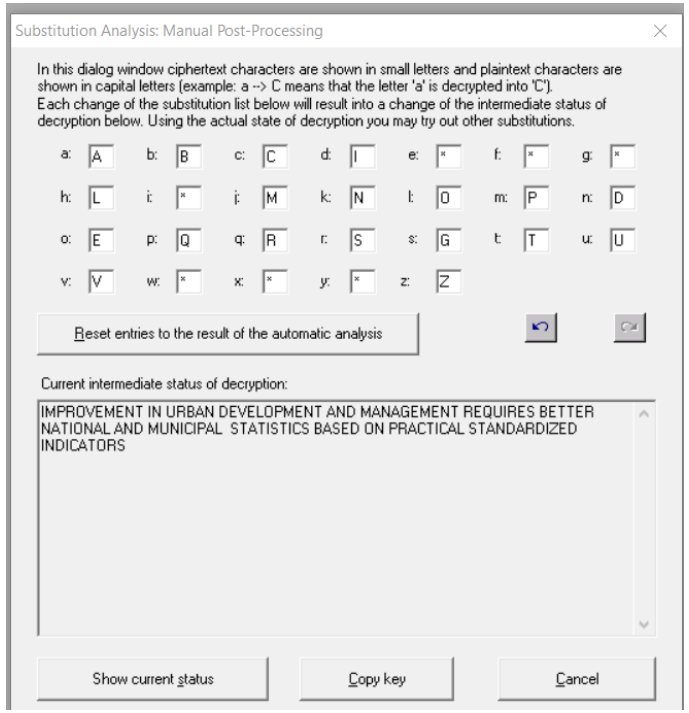
Задание 7-9

Для коротких текстов (менее 300 символов) можно использовать инструменты для ручной расшифровки.

Была совершена попытка ручного дешифрования для текстов. В первом случае проблема была в том, что не все символы встречаются в небольшом тексте, из-за этого не вся таблица замен была разгадана.

Во втором случае удалось отгадать всю таблицу, тк все символы в тексте встречались.





Основные характеристики шифра

Тип шифра: замена.

Ключ: кодовое слово и смещение.

Сложность атаки “грубой силы” составляет O(n!), где n - мощность алфавита

Шифр Permutation/Transposition

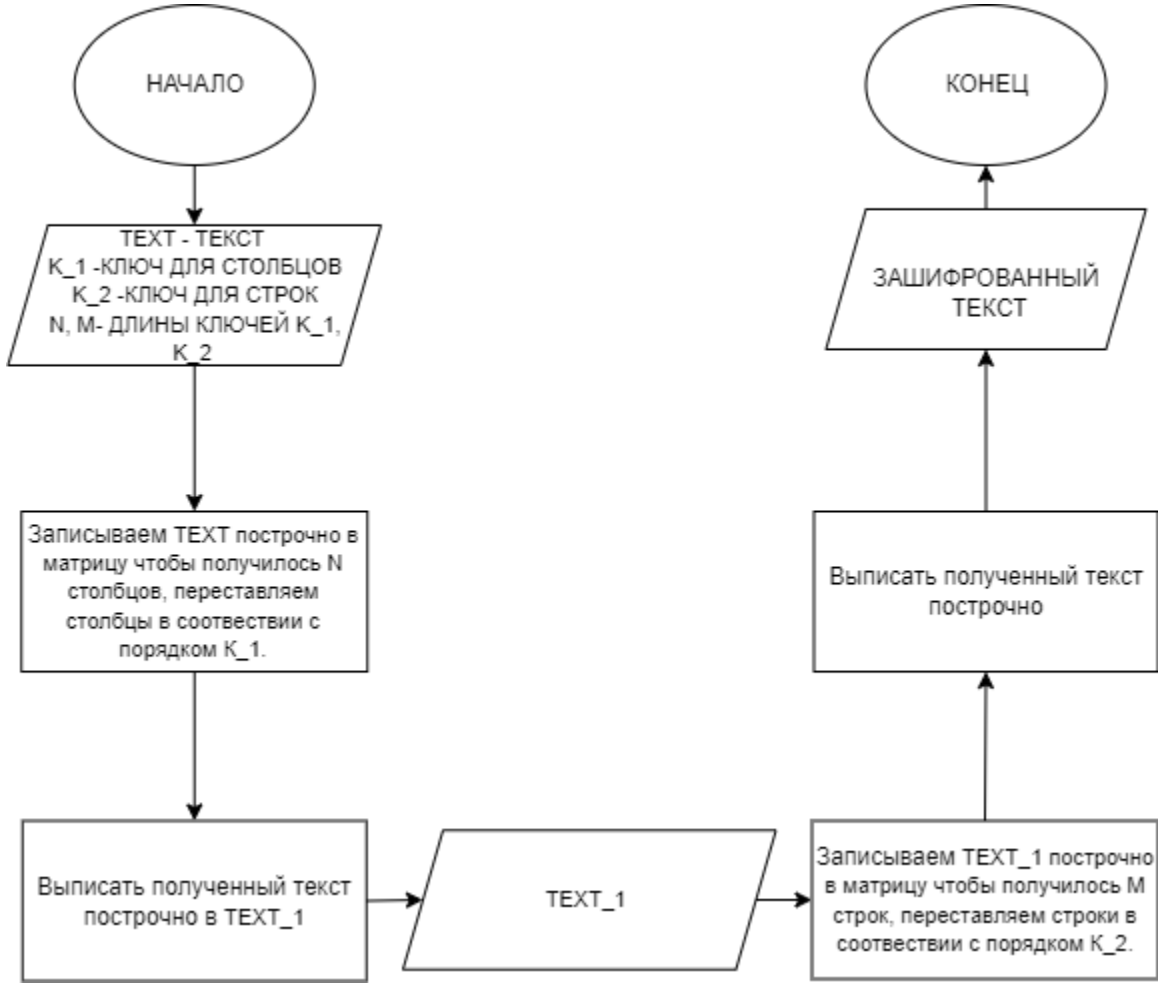
Задание

1. Найти шифр в CrypTool 1: Encrypt/Decrypt –> Symmetric(Classic).
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.
5. Выполнить самостоятельную работу:

а) зашифровать текст с произвольным сообщением в формате «DEAR message THANKS», используя только одинарную перестановку. Обменяться подобными шифровками с коллегой по учебной группе для дешифровки при условии, что формы обращения и завершения письма известны;

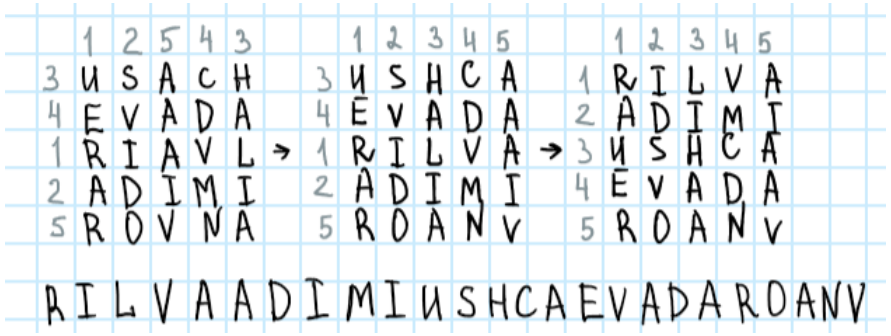
б) самостоятельно изучить атаку, реализованную в CrypTool 2, опираясь на Help и ссылки на статьи.

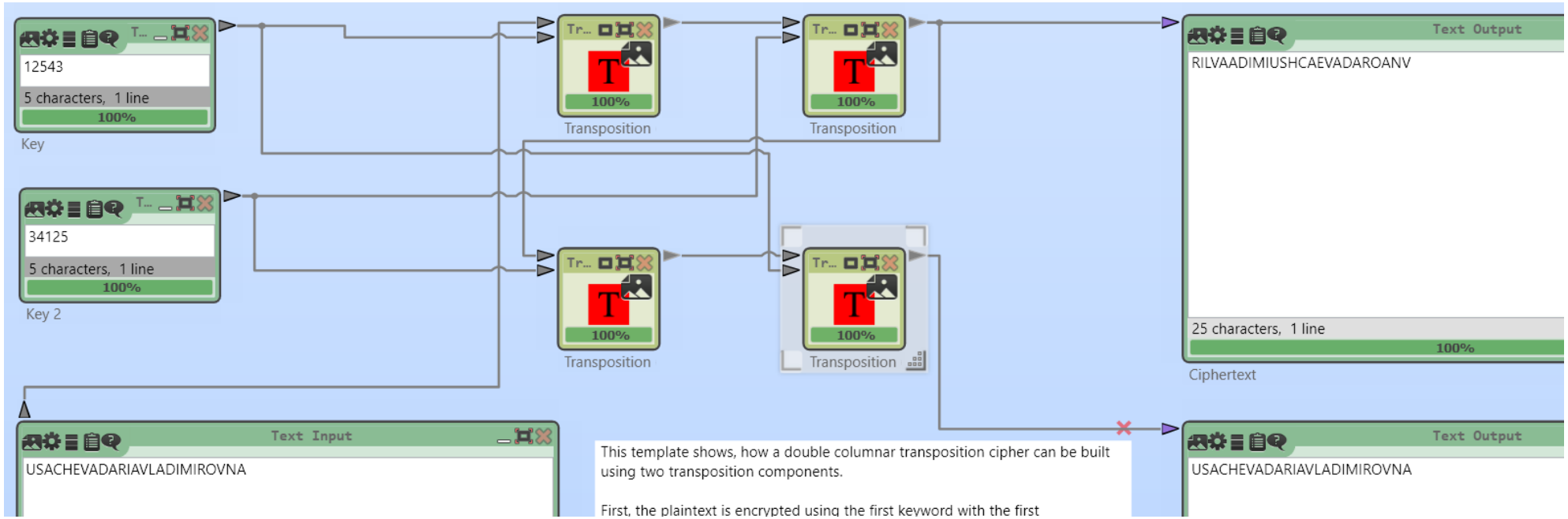
Схема алгоритма зашифрования сообщения



Задание 1-2

Текст был зашифрован и расшифрован вручную и с помощью CrypTool 2 (чтение и вывод по строкам, перестановка сначала по столбцам потом по строкам). Результаты совпадают.





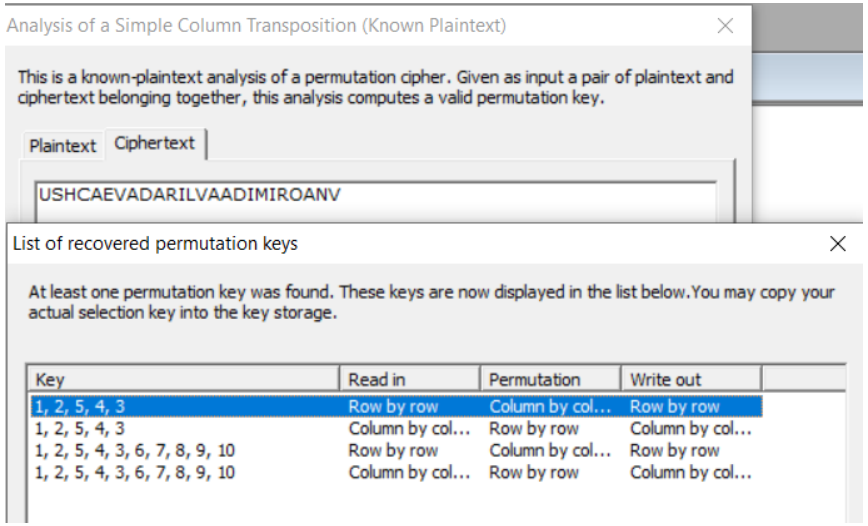
Задание 3

После выполнения зашифрования и расшифрования с различными ключами и вариантами перестановки матрицы с текстом было установлено, как работают параметры утилиты:

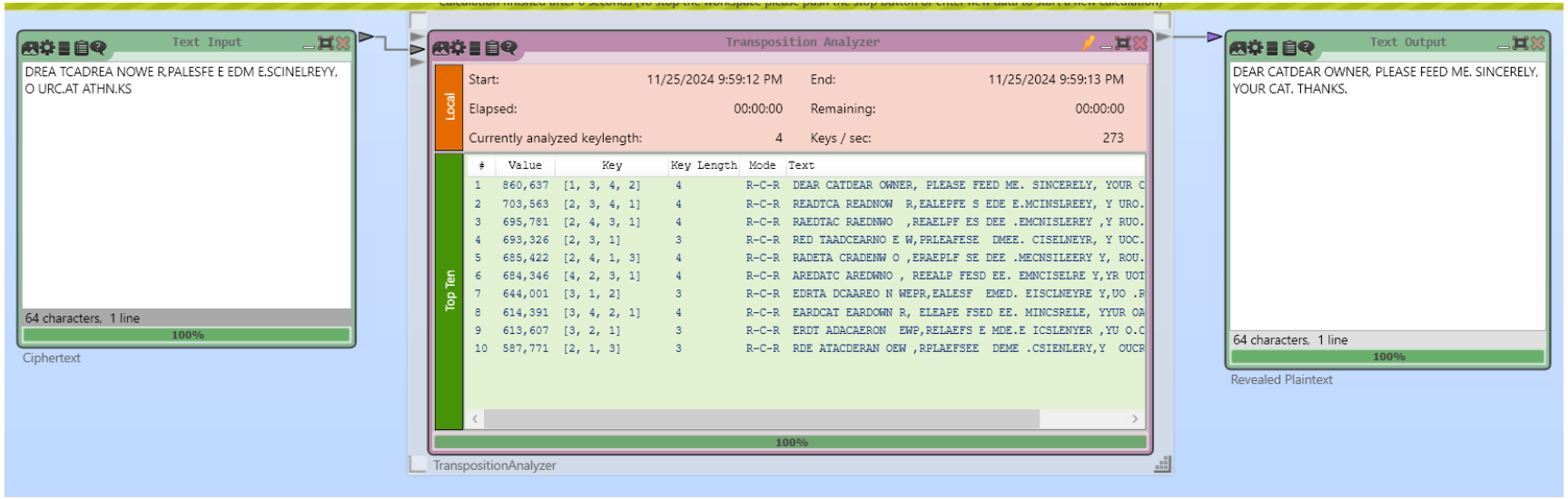
1. Выбираются параметры считывания и вывода по строке (слева направо) или по столбцу (сверху вниз);
2. Ключ – параметр для перестановки строк или столбцов (в зависимости от выбора пользователя). Ключом может быть как последовательность чисел так и букв.

Задание 4-5

Была проведена атака, основанная на знании исходного текста, в программе Cryptool 1. Полученный в результате атаки ключ оказался подходящим для дешифровки.



Была изучена атака в программе Cryptool 2, результат дешифровки совпадает с исходным текстом.



Основные характеристики шифра

Тип шифра: перестановка.

Ключ: ключ для перестановки строк и ключ для перестановки столбцов.

Сложность атаки “грубой силы” составляет O(n!*m!), где n и m – количество строк и столбцов соответственно.

Шифр Vigenere

Задание

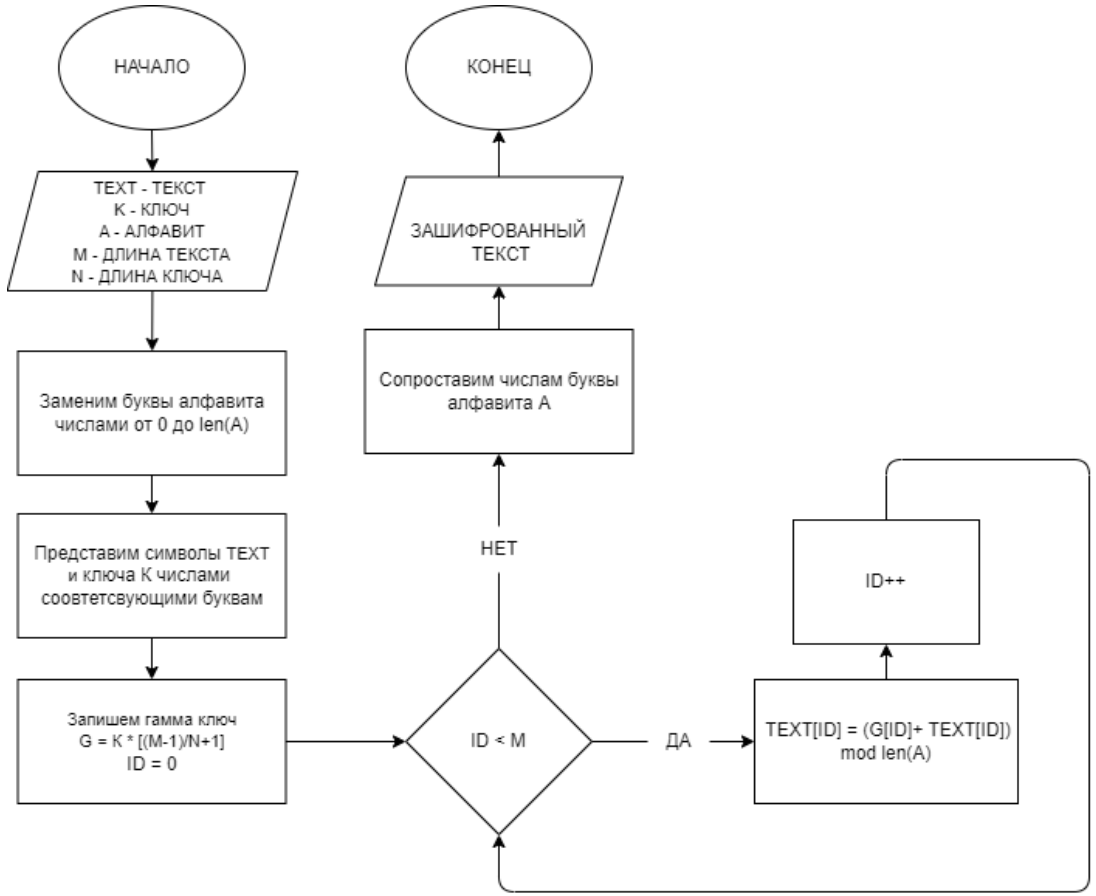
1. Найти шифр в CrypTool 1: Encrypt/Decrypt –> Symmetric(Classic).
2. Зашифровать и расшифровать текст, содержащий только вашу фамилию (транслитерация латиницей), вручную и с помощью шифра с выбранным ключом. Убедиться в совпадении результатов.
3. Провести атаку на шифротекст, используя приложение Analysis –> 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;

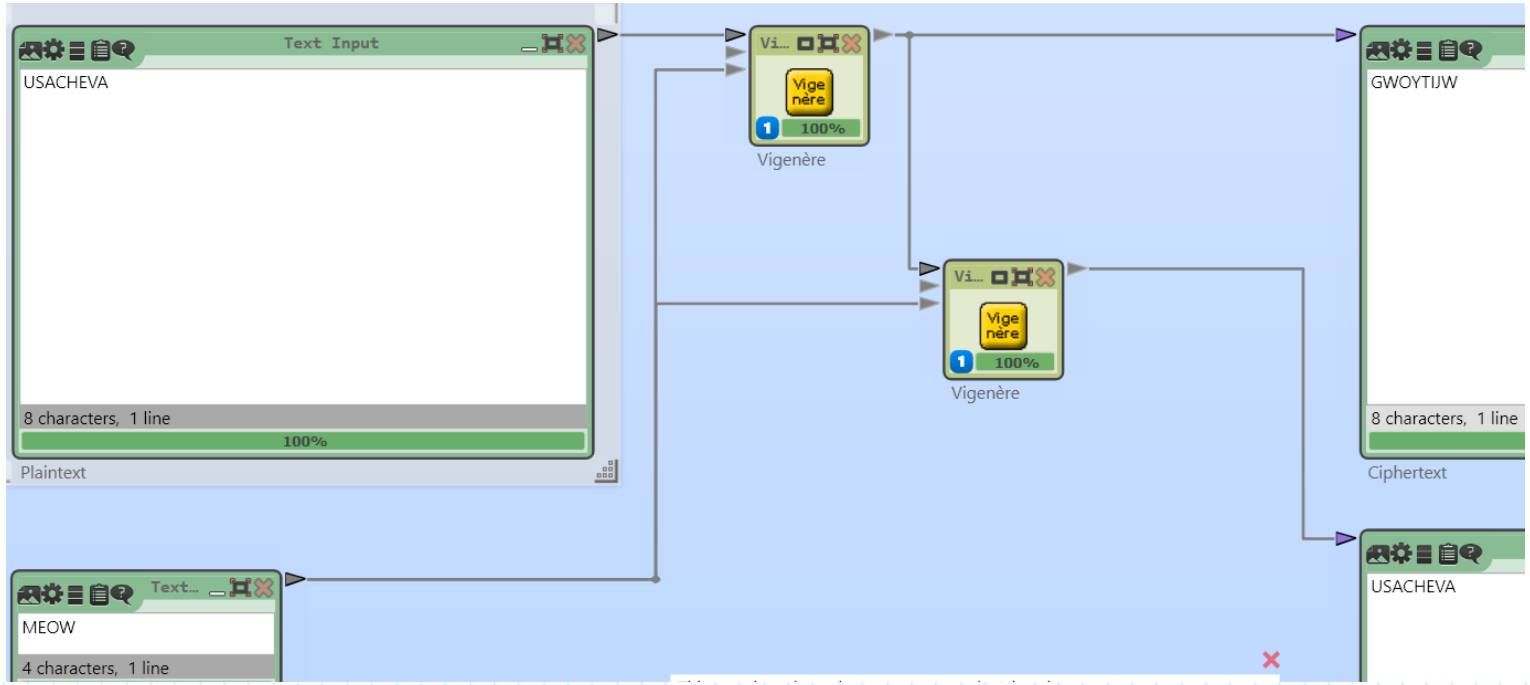
   в) определить очередную букву ключа приложением Analysis –> Symmetric Encryption(Classic) –> Cipher Text Only –> Caesar.
6. Выполнить самостоятельную работу: изучить атаку, реализованную в CrypTool 2, опираясь на Help и ссылки на статьи.

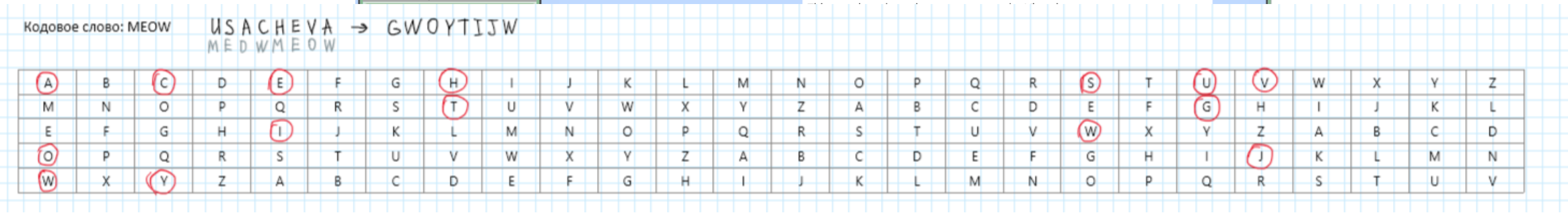
Схема алгоритма зашифрования сообщения



Задание 1-2

Текст был зашифрован и расшифрован вручную и с помощью CrypTool 2. Результаты совпадают.

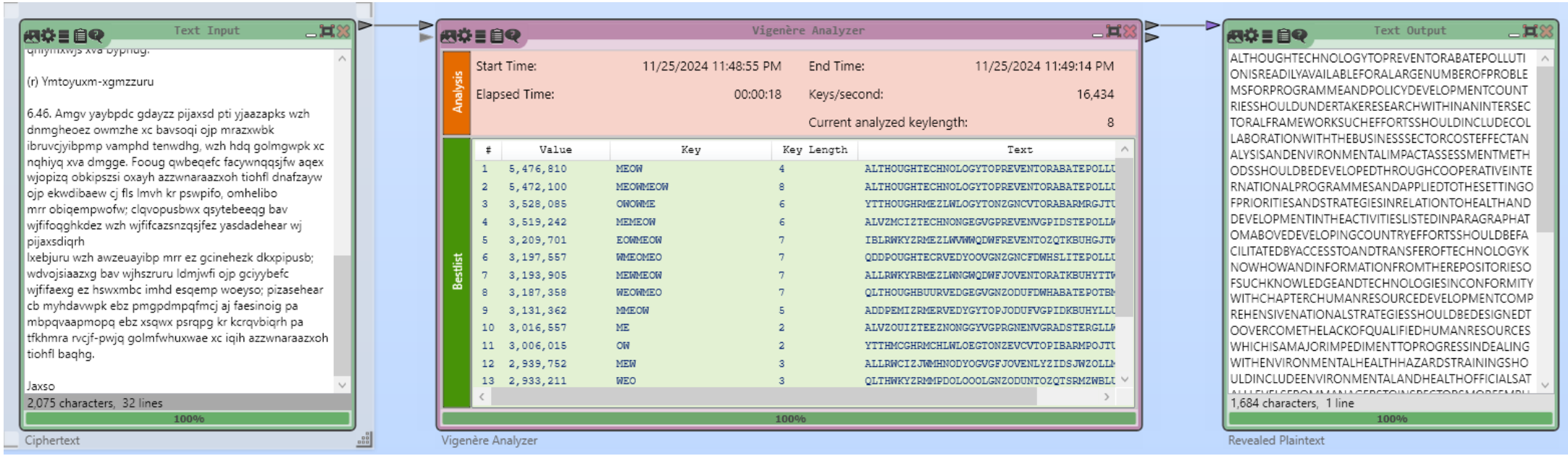




A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

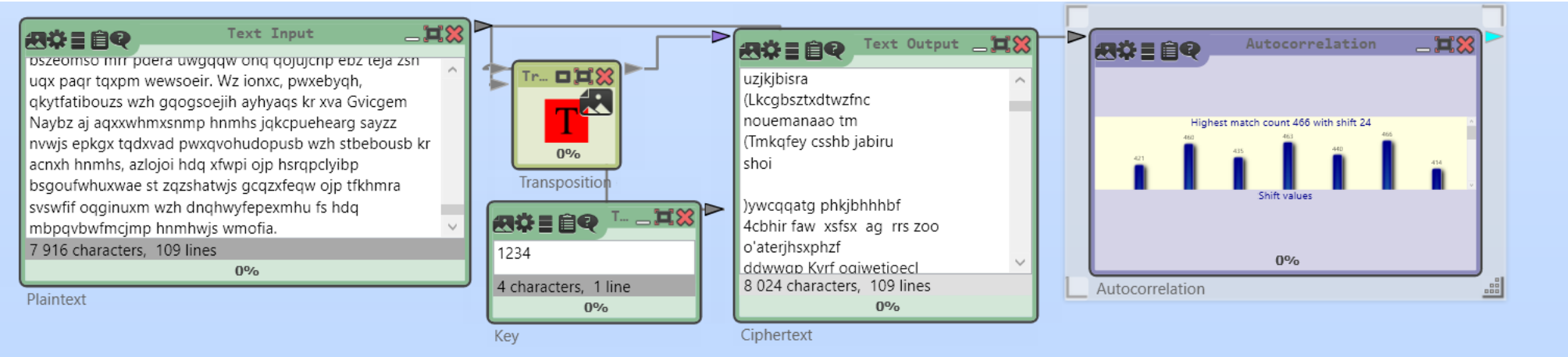
Задание 3-4

Была проведена атака на фрагмент шифротекста из English.txt в программе Cryptool 2. Полученное в результате атаки ключевое слово “MEOW” оказалось верным.



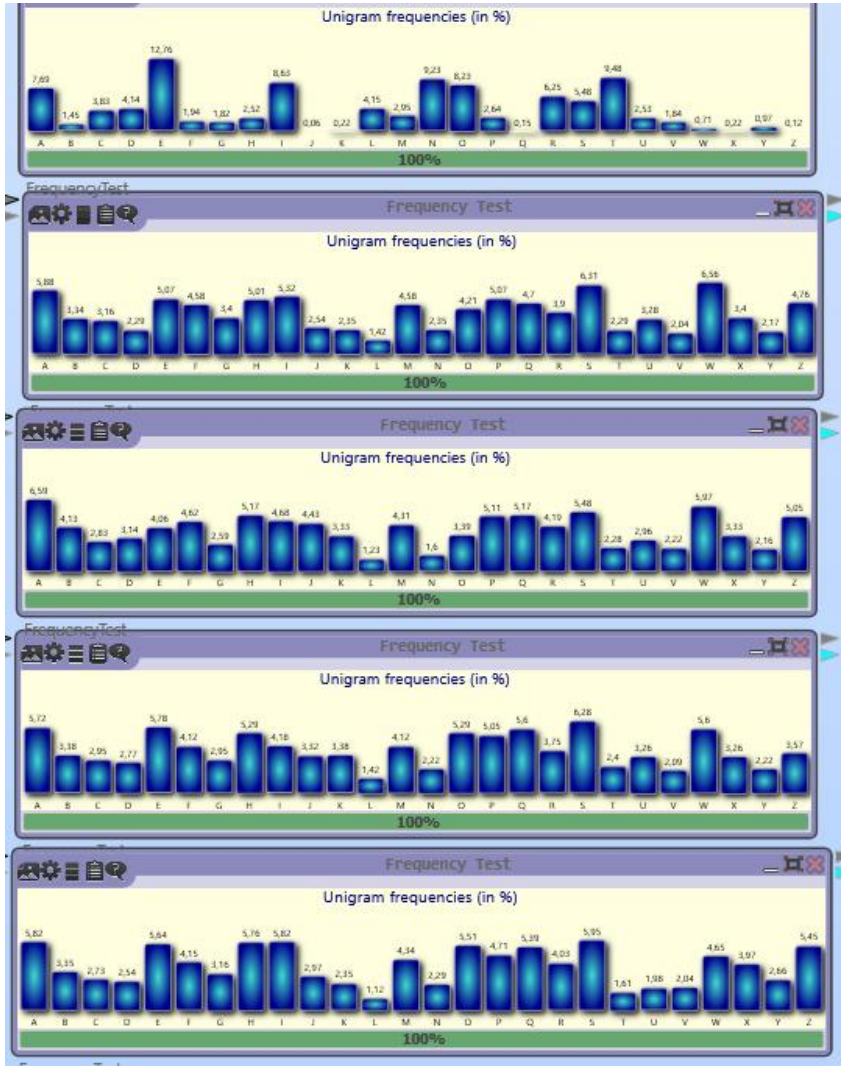
Задание 5(а,б)

С помощью автокорреляционного метода, была получена гистограмма. По пикам можно сделать вывод, что размер ключа кратен или равен 4. Была совершена перестановка текста с размером столбца 4



Задание 5(в)

Текст был разделен на 4 части, каждая из которой представляет собой текст, зашифрованный шифром Цезаря, нужно проанализировать частоту встречи букв и сравнить с исходной гистограммой частот. Проанализировав гистограммы, был получен следующий результат: 1 –> M, 2 -> E, 3 -> O, 4 -> W/



Основные характеристики шифра

Тип шифра: замена.

Ключ: кодовое слово.

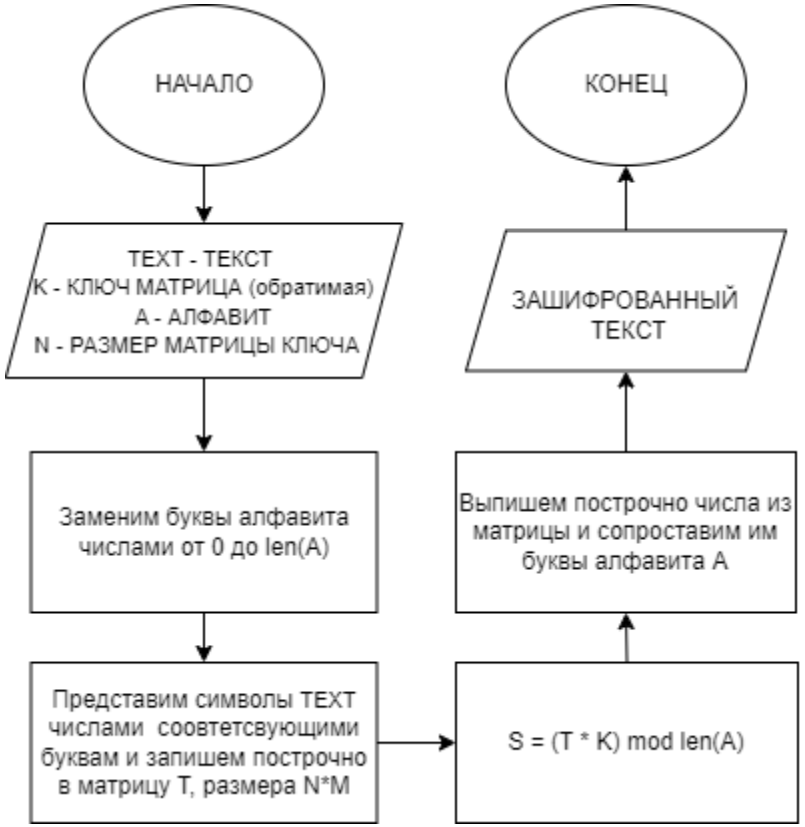
Сложность атаки “грубой силы” составляет O($\frac{n!}{(n-m)!}$), где n – мощность алфавита, а m – длина ключа.

Шифр Hill

Задание

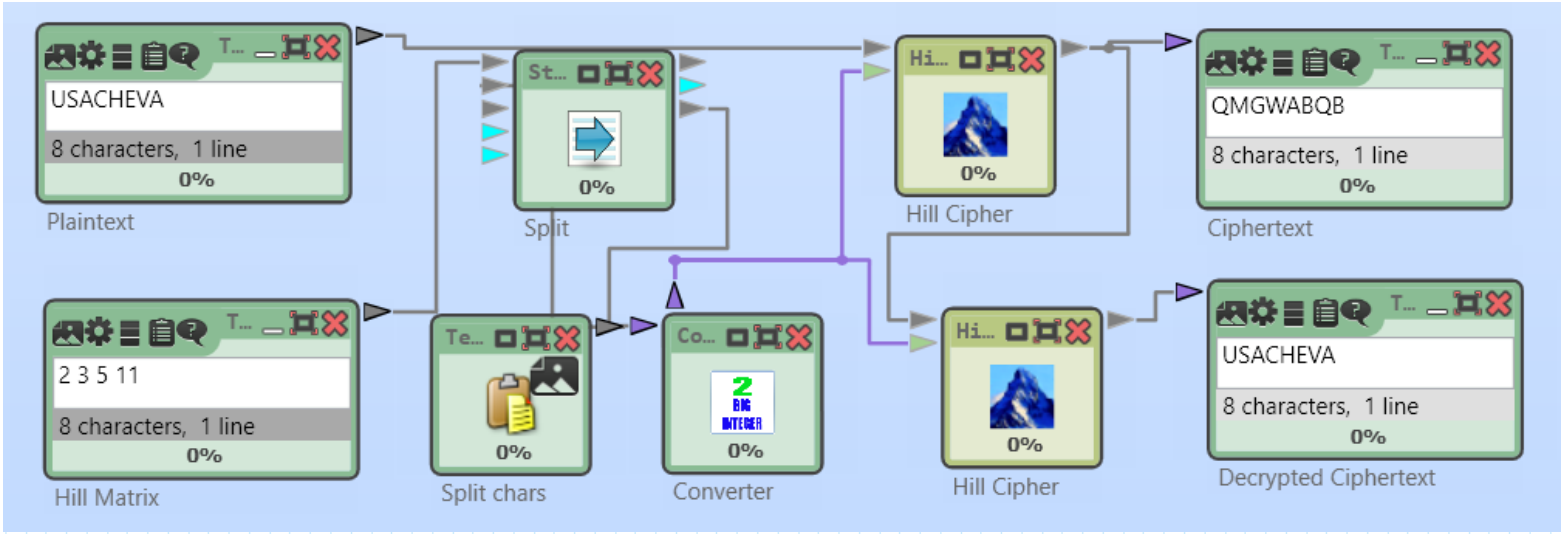
1. Найти шифр в CrypTool 1: Encrypt/Decrypt –> Symmetric(Classic).
2. Зашифровать и расшифровать текст, содержащий только вашу фамилию (транслитерация латиницей), вручную и с помощью шифра с выбранным ключом 2 × 2. Убедиться в совпадении результатов. Проверить обратимость шифрующей матрицы (ключа).
3. Зашифровать текст с произвольным сообщением в формате «DEAR MR 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.
5. Выполнить самостоятельную работу: обменяться шифровками с коллегой по учебной группе для дешифрования при условии, что формы обращения и завершения сообщения известны. Размерность использованного ключа держать в секрете.

Схема алгоритма зашифрования сообщения



Задание 1-2

Текст был зашифрован и расшифрован вручную и с помощью CrypTool 2. Результаты совпадают.



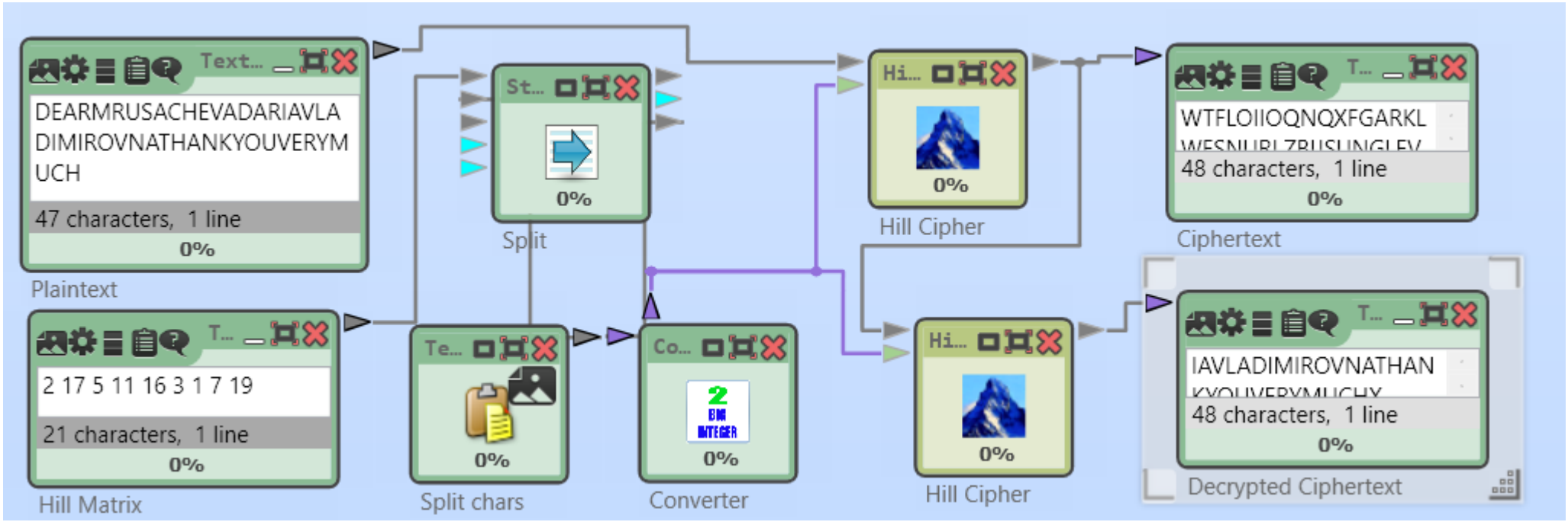
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

20	18		Ключ				94	298		16	12														
0	2	×	2	5	=		6	22	=	6	22	mod 26	→	Q	M	G	W	A	B	Q	B				
7	4		3	11			26	79		0	1														
21	0						42	105		16	1														

2	5	-1	9	3	mod 26		16	12					228	96		20	18								
3	11	=	7	4			6	22	×	9	3	=	208	106	=	0	2	mod 26							
							0	1		7	4		7	4		7	4								
							16	1					151	52		21	0								

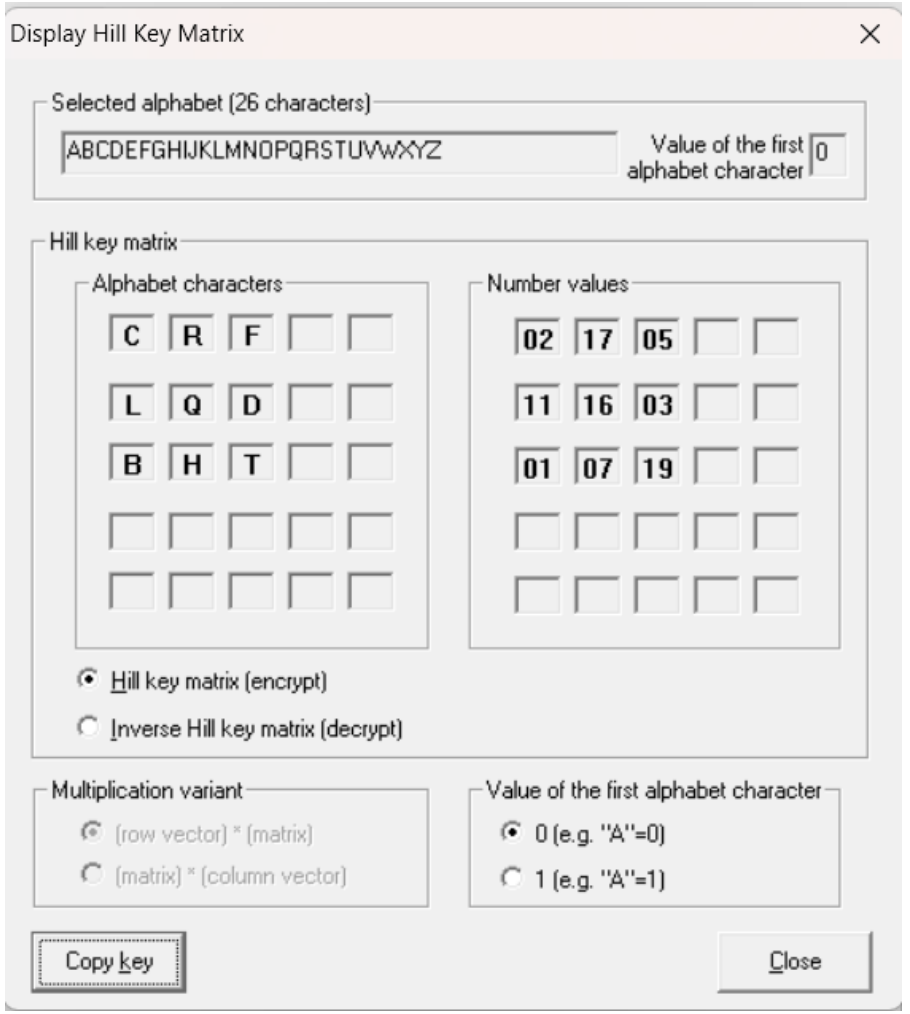
Задание 3

Был зашифрован текст DEAR MR USACHEVA DARIA VLADIMIRONA THANK YOU VERY MUCH с шифрующей матрицей размером 3 на 3.



Задание 4

Была проведена атака, основанная на знании исходного текста, в программе Cryptool 1. Полученный в результате атаки ключ оказался верным.



Основные характеристики шифра

Тип шифра: замена.

Ключ: матрица шифрования (обратимая).

Сложность атаки “грубой силы” составляет O(n^{m*m}), где n – количество строк матрицы с текстом, а m – размер матрицы шифрования.

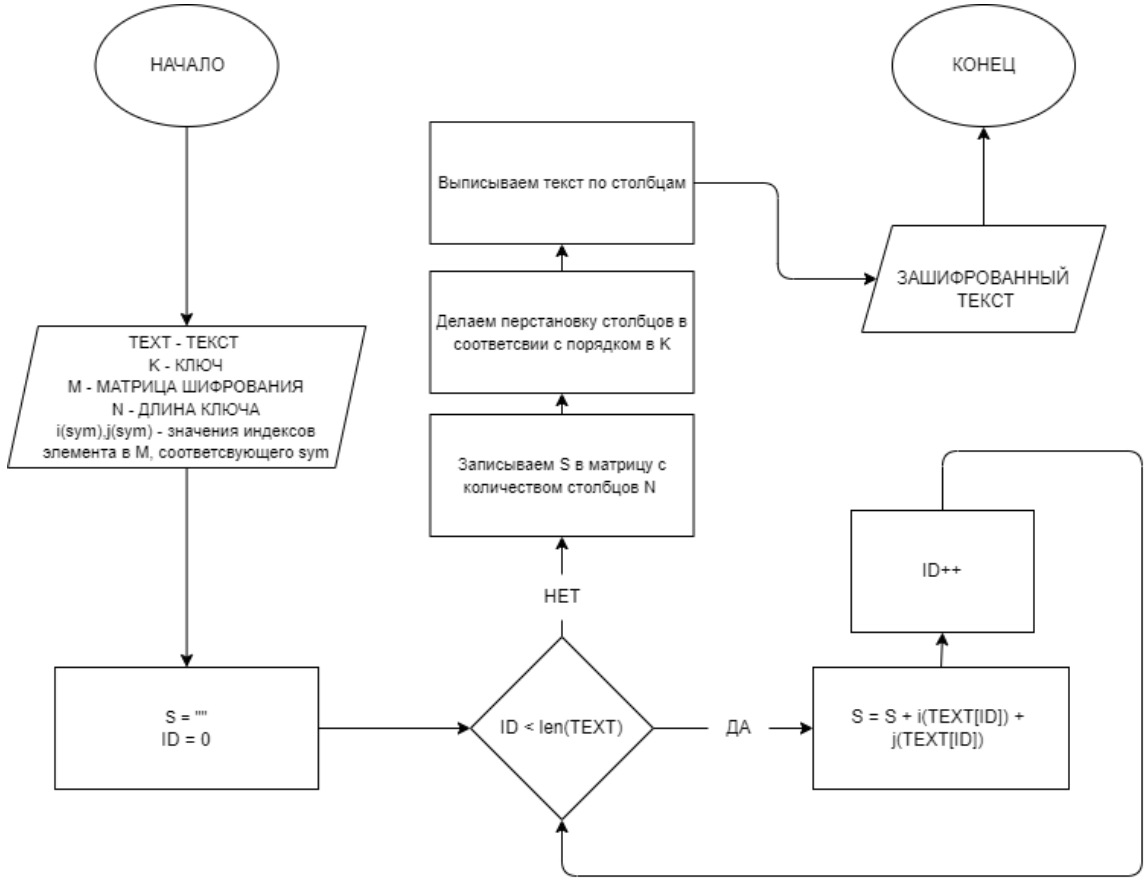
Шифр Adfgvx

Задание

1. Найти шифр в CrypTool 1: Encrypt/Decrypt –> Symmetric(Classic).
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.
7. Выполнить самостоятельную работу:

а) зашифровать текст из 200 символов, сохранить ключ, и обменяться шифровками с коллегой по группе для дешифровки; б) самостоятельно изучить атаку по словарю, реализованную в CrypTool 2, опираясь на Help и ссылки на статьи.

Схема алгоритма зашифрования сообщения



Задание 1-2

Текст был зашифрован и расшифрован вручную и с помощью CrypTool 2.

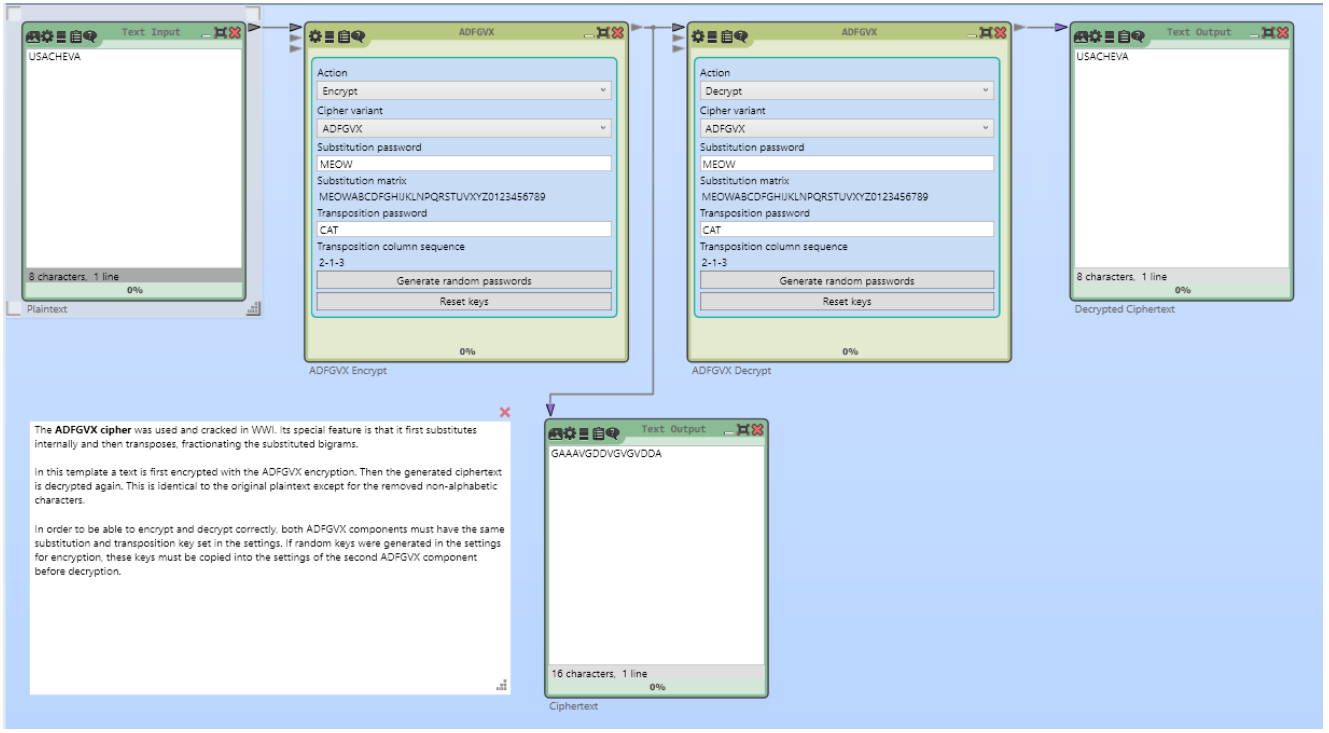
Результаты совпадают.

USACHEVA = GGGDAVDADVADGVAV = GAAAVGDDDGVGVVVVA

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

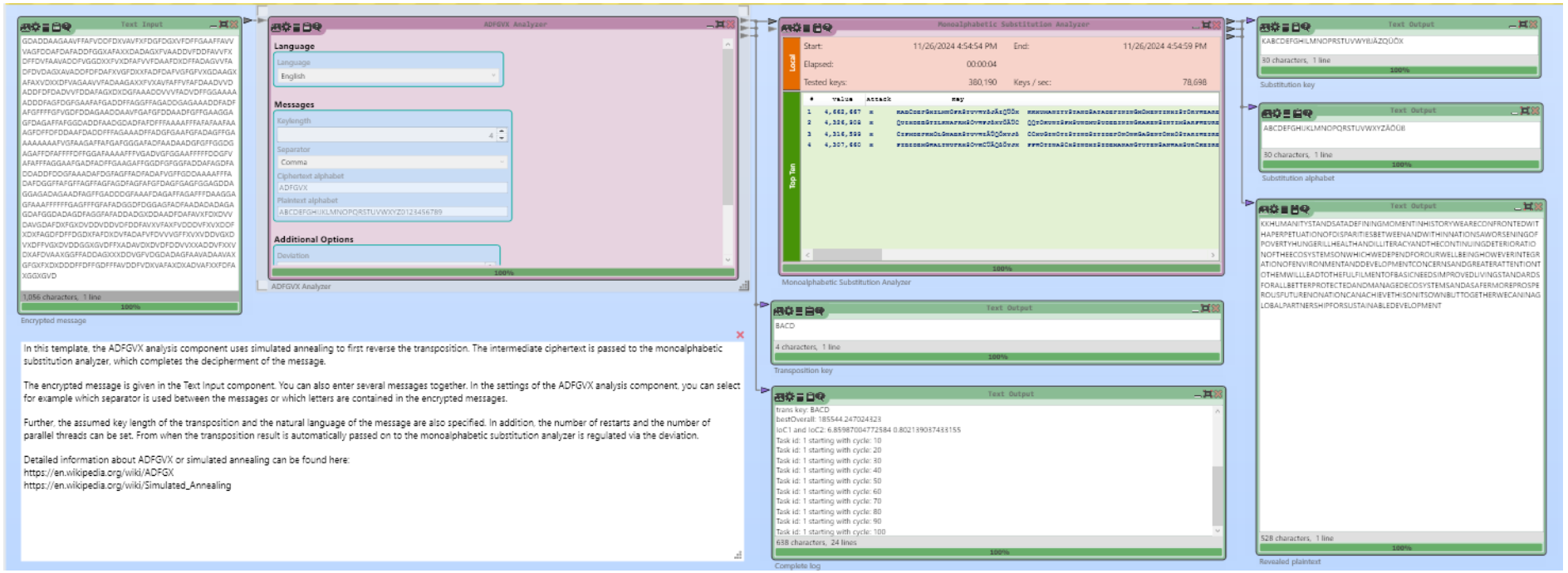
C	A	T
G	G	G
D	A	V
D	A	V
D	A	V
G	V	A
V		

A	C	T
G	G	G
A	D	V
A	D	V
A	D	V
V	G	A
	V	

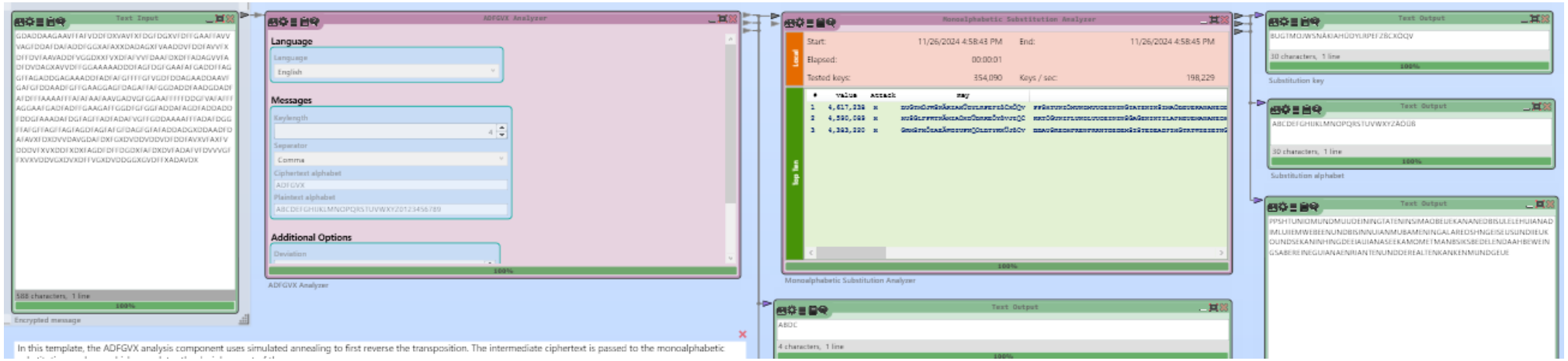


Задание 3-5

Взяты и зашифрованы 3 абзаца по 600, 300, 150. Выполнены атаки на шифротекст. Как можно заметить, исходный текст совпадает с результатом атаки для 600 символов. Для 300 символов текст расшифрован частично верно. Для 150 символов текст расшифрован неверно, так как он слишком короткий.



Задание 3-5

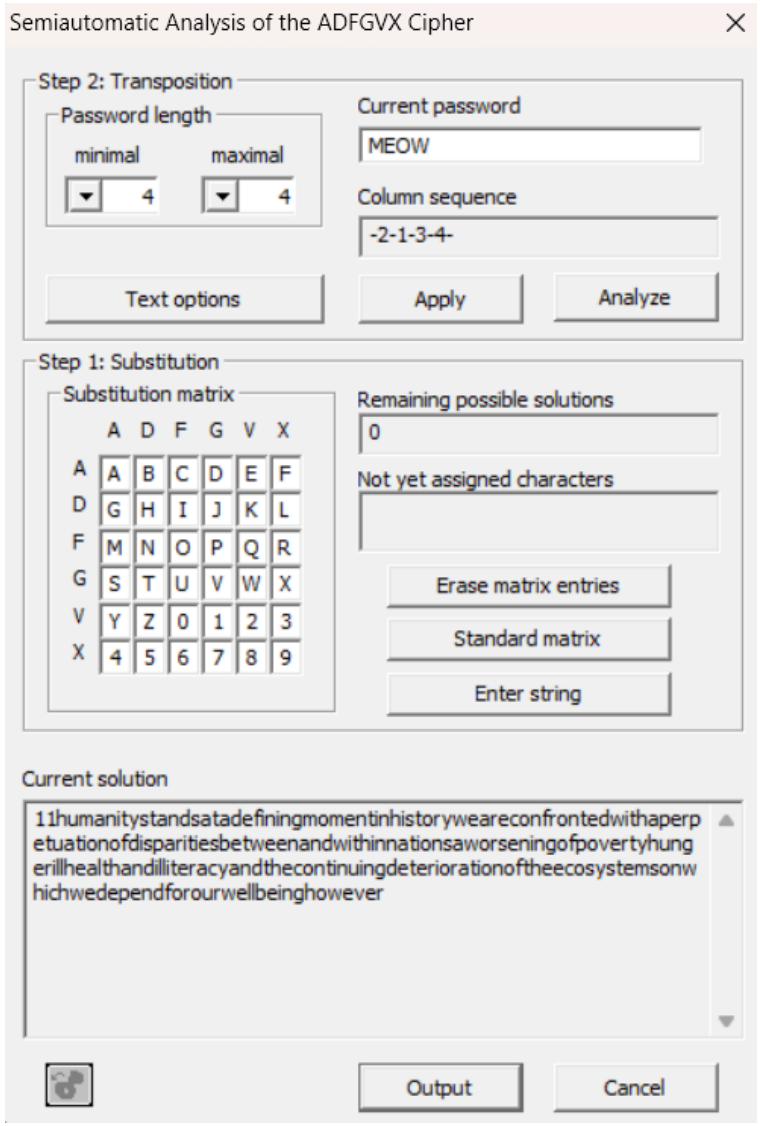

Text Input
ADFGVX Analyzer
Language
Messages
Additional Options
Monoalphabetic Substitution Analyzer
Text Output
In this template, the ADFGVX analysis component uses simulated annealing to first reverse the transposition. The intermediate ciphertext is passed to the monoalphabetic


Text Input
ADFGVX Analyzer
Language
Messages
Additional Options
Monoalphabetic Substitution Analyzer
Text Output

Задание 6

Был изучен инструмент автоматизации ручного расшифрования для текстов менее 300 символов.

С помощью данной утилиты можно перебрать все варианты ключей, если известно смещение алфавита, а также лучше знать приблизительную длину ключа, что ускорит дешифрование текста



Основные характеристики шифра

Тип шифра: комбинированный.

Ключ: кодовое слово и матрица шифрования.

Сложность атаки “грубой силы” составляет O(36!*n!), где n – длина ключа.

Заключение

1. Шифр Scytale:

Этот шифр использует перестановку символов, где ключом служат количество граней цилиндра и значение отступа.

Его сложность атаки грубой силой оценивается в O(n^2), учитывая две переменные - количество граней и смещение.

2. Шифр Caesar:

Данный шифр основан на простом сдвиге букв по алфавиту, где ключом является величина этого сдвига.

Сложность атаки грубой силы оценивается в O(n), где n - размер алфавита.

3. Шифр Substitution:

Этот шифр представляет собой шифр замены, использующий ключевое слово и значение сдвига.

Сложность атаки грубой силой оценивается в O(n!).

4. Шифр Permutation/Transposition:

Шифр использует два ключевых слова для перестановки символов.

Сложность атаки грубой силы составляет O(n!*m!), где n и m – количество строк и столбцов соответственно.

5. Шифр Vigenere :

Этот шифр использует соответствие между открытым символом и несколькими закрытыми символами, основанный на порядке букв в алфавите, к которому применяется ключевое слово..

Сложность атаки грубой силы составляет O($\frac{n!}{(n-m)!}$), где n – мощность алфавита, а m – длина ключа.

6. Шифр Hill:

Шифр использует замену на основе матрицы шифрования(обратимой) как ключа.

Сложность атаки грубой силы составляет O(n^{m*m}), где n – количество строк матрицы с текстом, а m – размер матрицы шифрования.

7. Шифр ADFGVX:

Этот комбинированный шифр использует строку-ключ для перестановки элементов промежуточного текста и матрицу для замены символов.

Сложность атаки грубой силы составляет O(36!*n!), где n – длина ключа.