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

Лабораторная работа № 1

Изучение классических шифров

Студент: Порошина Алина Романовна, группа 0361

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

Санкт-Петербург 2024

Цель работы

Исследовать шифры:

1. Scytale
2. Caesar
3. Substitution
4. Permutation/Transposition
5. Vigenere
6. Hill
7. ADFGVX

И получить практические навыки работы с ними, в том числе с использованием приложения CrypTool 1 и 2.

Шифр «Сцитала»

Задание

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

2. Создать файл с открытым текстом, содержащим последовательность цифр. Рис. 1.15

3. Запустить шифр и выполнить зашифровку и расшифровку созданного текста несколько раз.

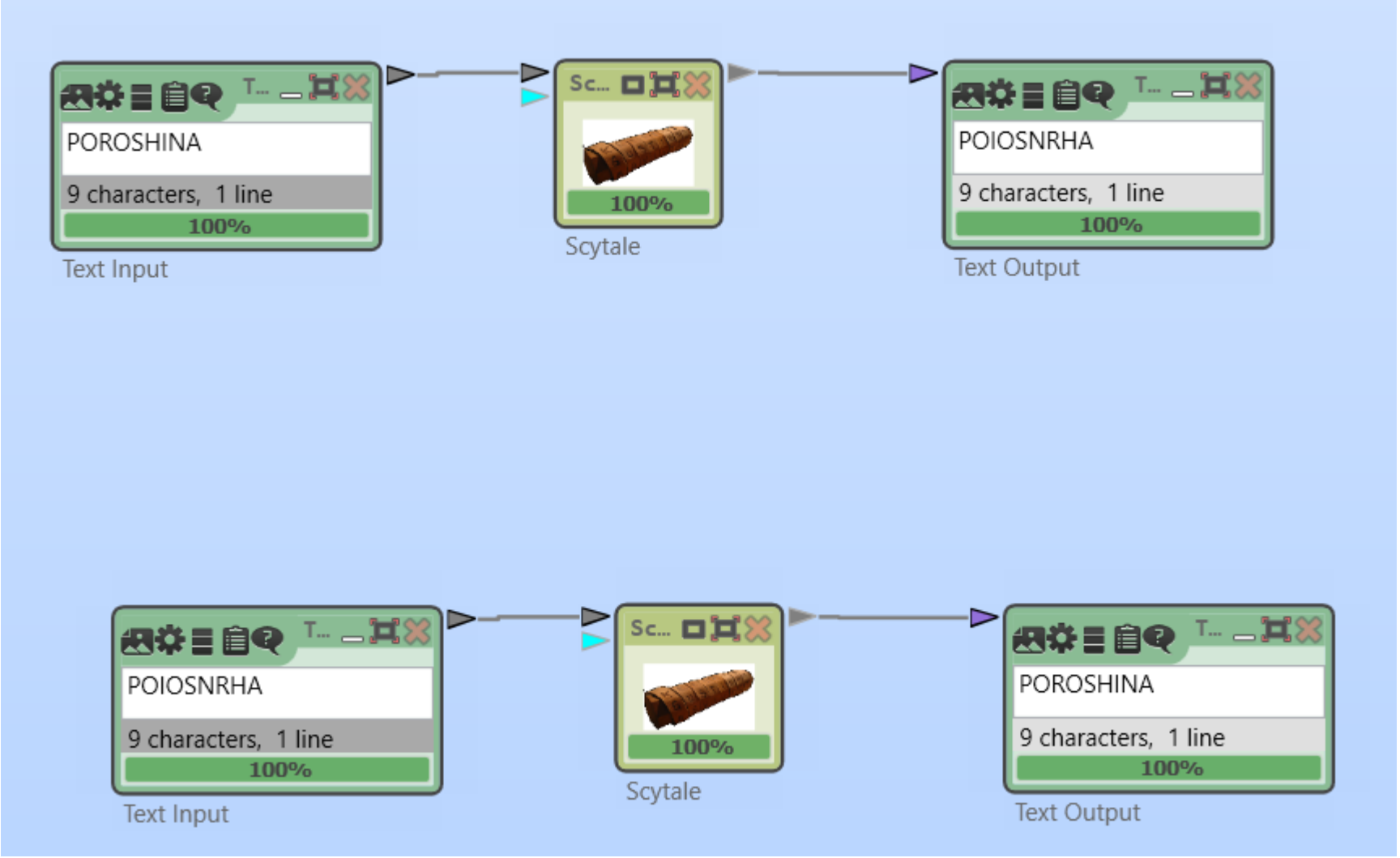
4. Установить, как влияют на шифрование параметры Number of Edges и Offset.

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.

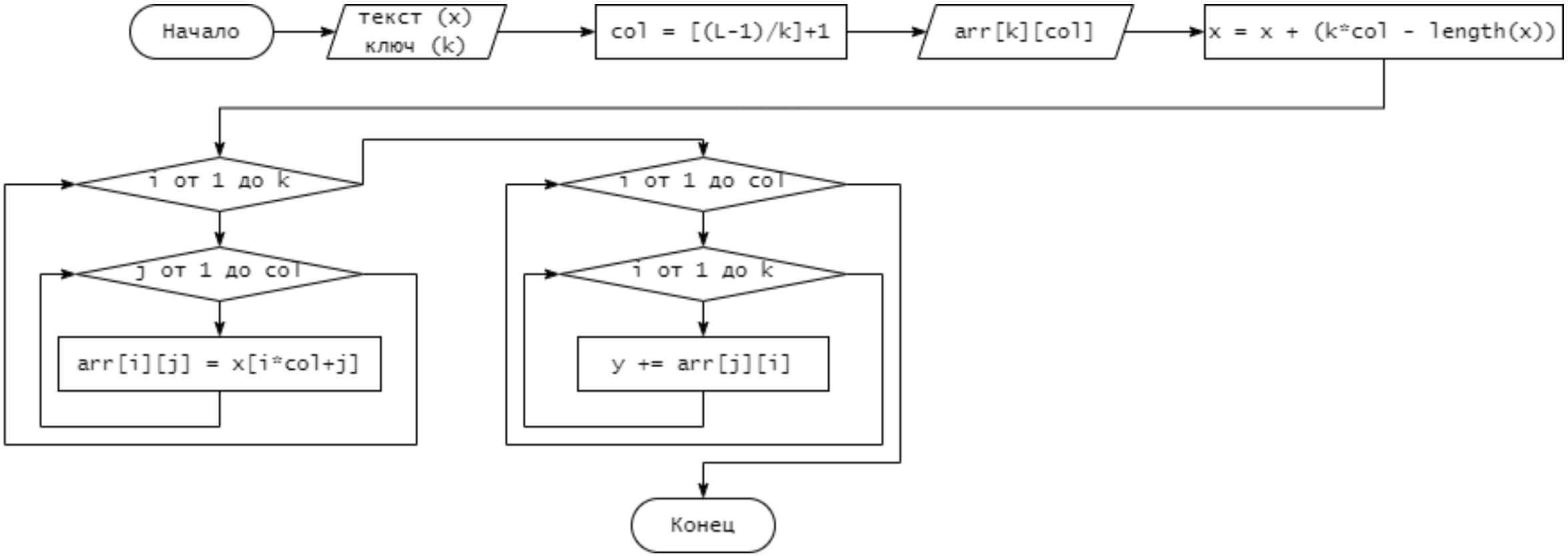
6. Выполнить самостоятельную работу: взять в CrypTool 2 шаблон атаки на шифр методом «грубой силы» и модифицировать этот шаблон, заменив блок с шифротекстом на блок ввода открытого текста и блок зашифрования.

Изучить принципы этой автоматической атаки.

Реализация в CrypTool 2



Схема, поясняющая работу шифра



Заключение

1. Был изучен шифр «Сцитала» и выявлены его следующие характеристики:

Шифр использует перестановку символов, где количество граней призмы служит в качестве ключа.

В ходе исследования была зашифрована и расшифрована фамилия вручную и с помощью программы CrypTool 2, и оба результаты совпали.

3. Была проведена атака «BruteForce» с помощью CrypTool 2. В результате путем анализа был составлен список потенциальных ключей, из которого был выбран правильный.

4. Была проведена оценка сложности атаки «BruteForce», здесь L – длина шифротекста:

Оценка при отсутствии сдвига – $O(L)$

Оценка со сдвигом – $O(L$^2)

Шифр Цезаря

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.

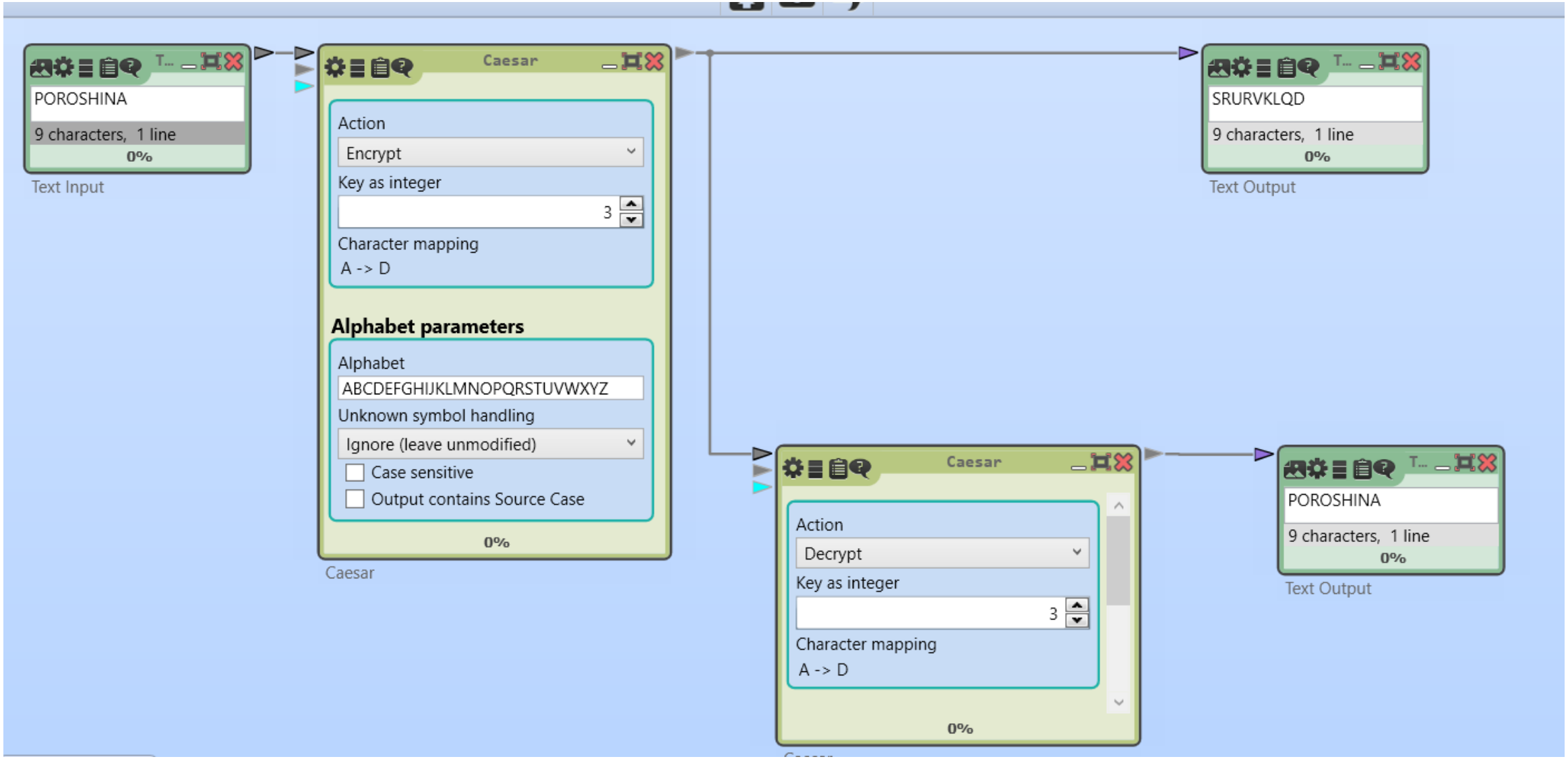
4. Зашифровать ключом отличным от 0 файл CrypTool-en.txt (папка CrypTool/Examples).

5. Построить гистограмму частот букв в зашифрованном тексте, сравнить визуально гистограммы и подтвердить ключ зашифрования.

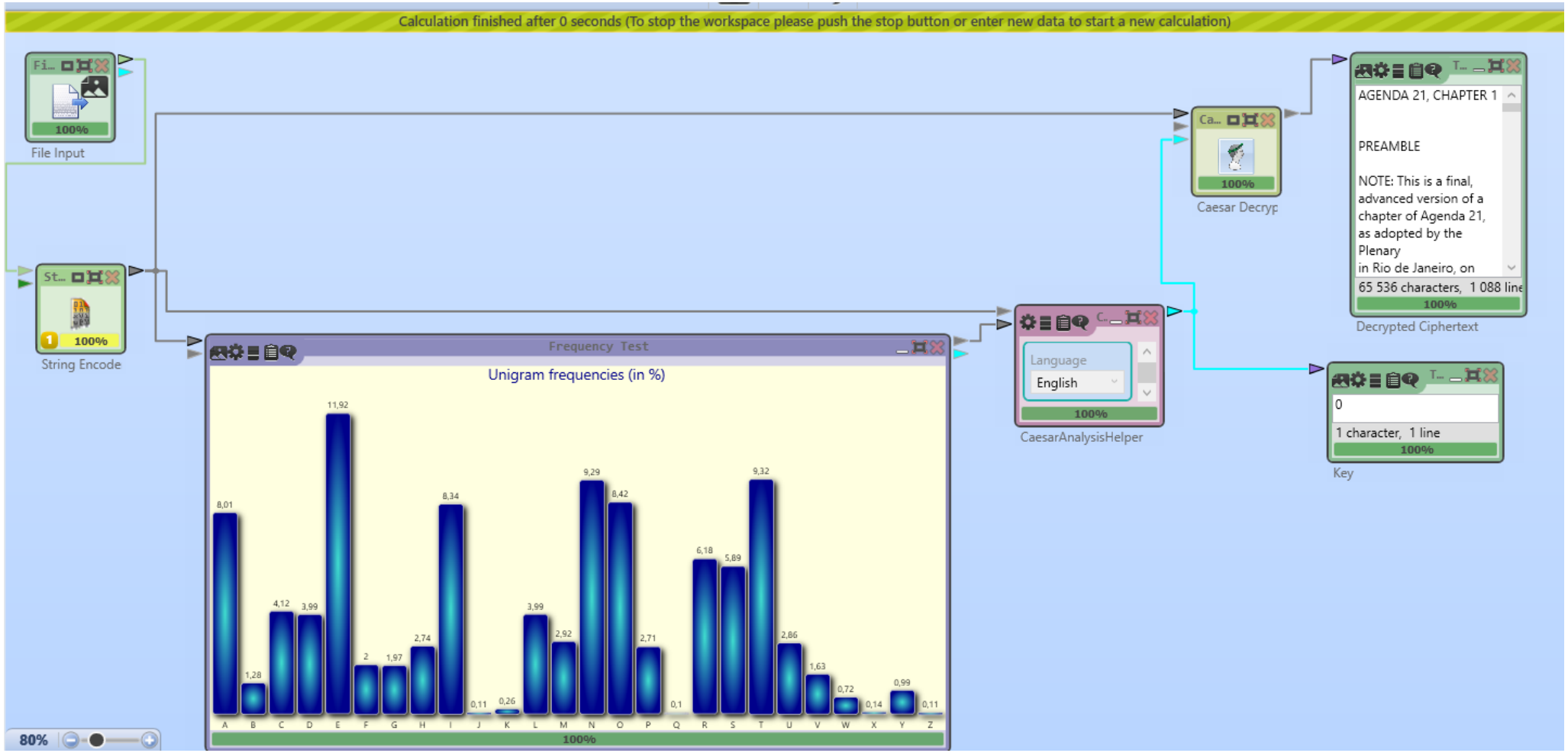
6. Проверить гипотезу о значении ключа утилитой Analysis –> Symmetric Encryption(Classic) –> Cipher Text Only –> Caesar.

7. Выполнить самостоятельную работу: обменяться шифровками с коллегой по группе для проведения подобной атаке по дешифрации сообщения.

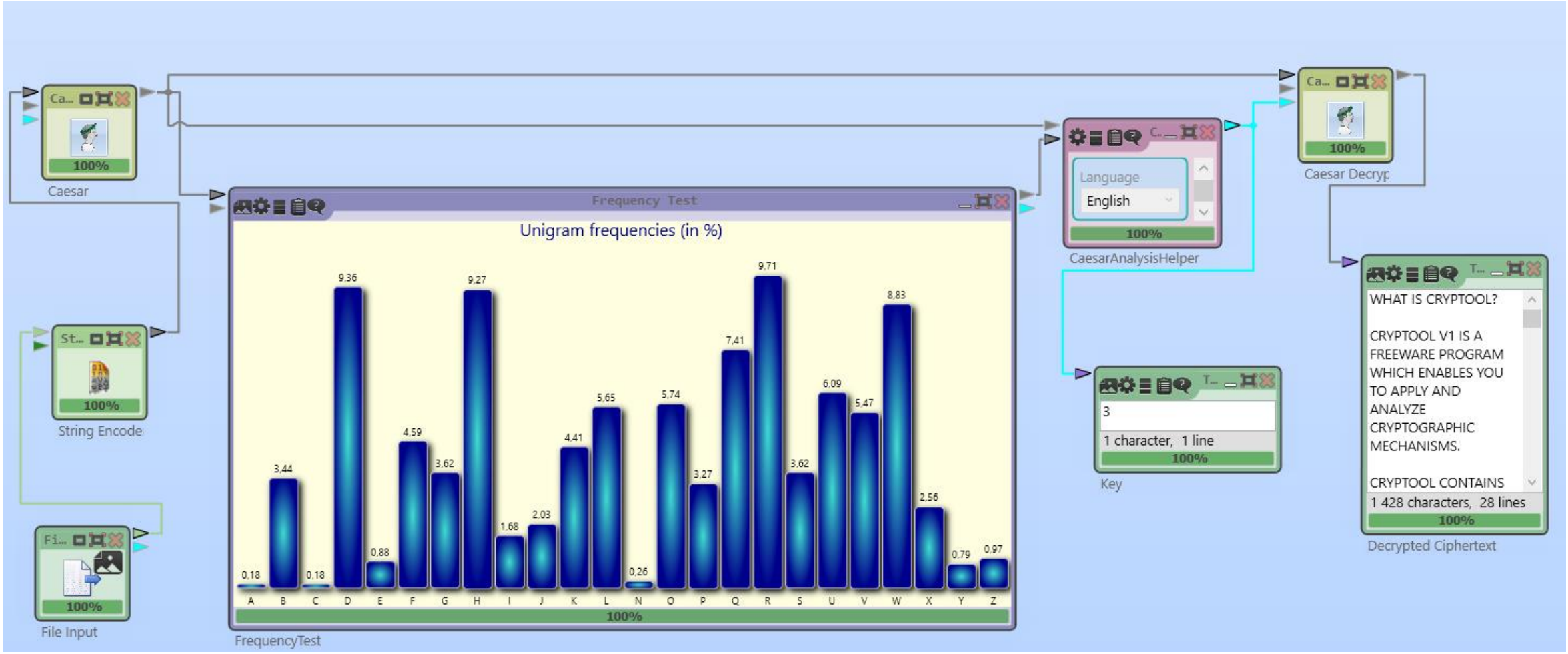
Реализация в CrypTool 2



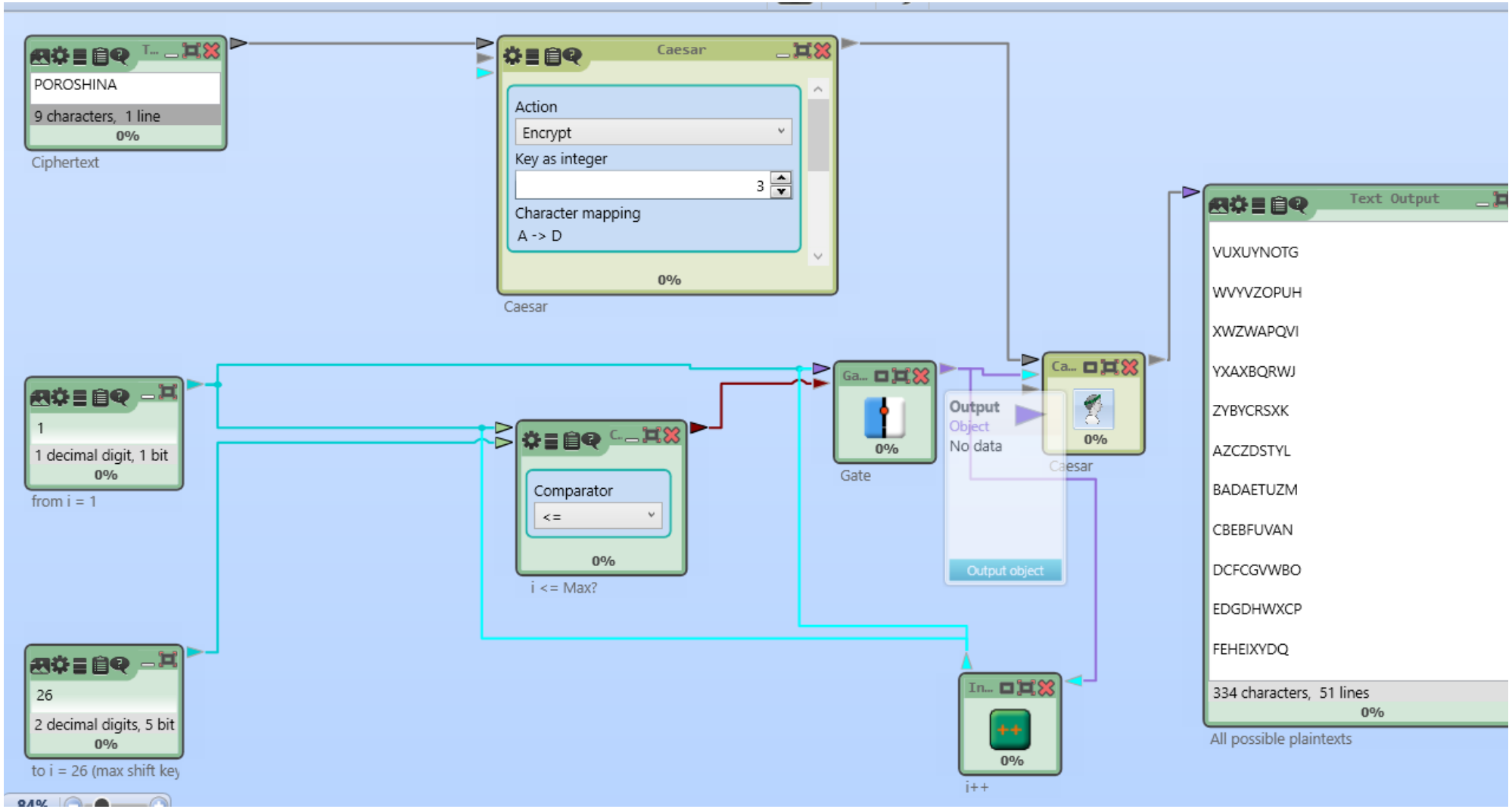
Гистограмма English.txt



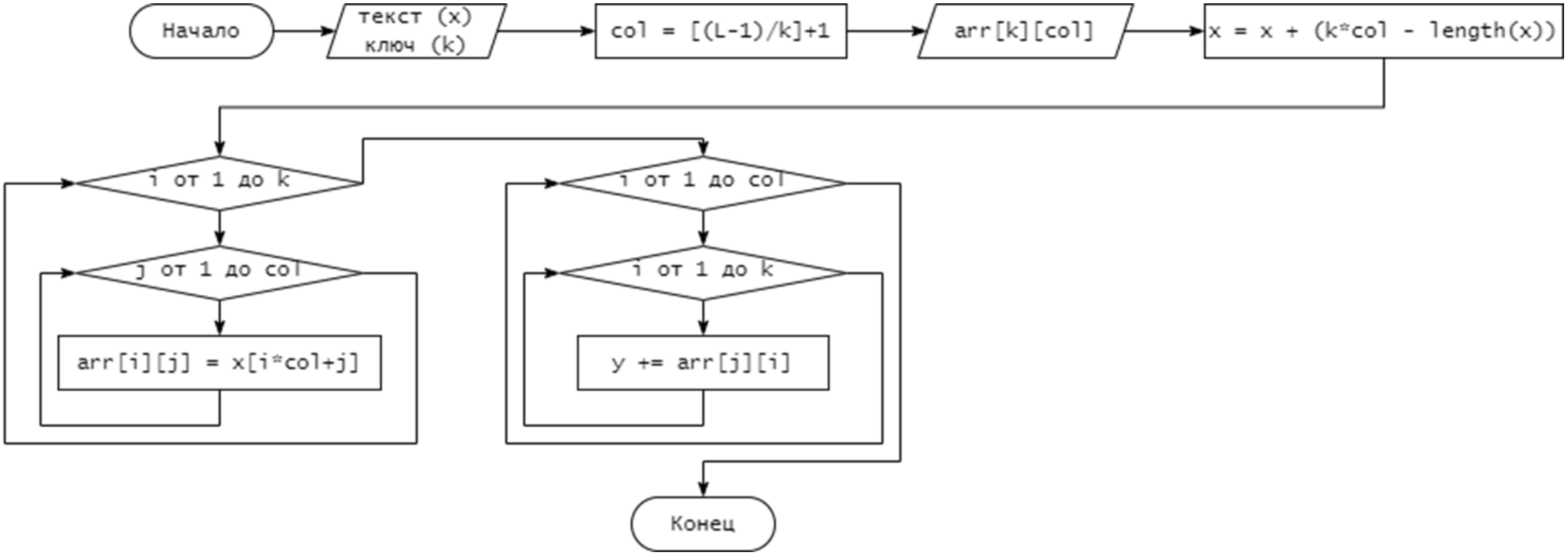
Гистограмма cryptool-en.txt



БрутФорс атака



Схема, поясняющая работу шифра



Заключение

1. Был изучен шифр «Цезарь» и выявлены его следующие характеристики :

Шифр представляет собой аддитивный шифр замены, где ключом является сдвиг.

В процессе исследования этого шифра была зашифрована и расшифрована фамилия как вручную, так и с использованием CrypTool 2. Оба результата совпали.

2. Была проведена атака методом "Frequency Analysis" с использованием программы CrypTool 2 на выборках из 10000 и 1000 символов. В первом случае был составлен список потенциальных ключей, среди которых был выбран правильный. Однако во втором случае атака оказалась недостаточно эффективной.

3. Была проведена оценка сложности атаки «BruteForce», здесь A – мощность алфавита:

Оценка – $O(A)$

Шифр моноалфавитной подстановки

Задача

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.

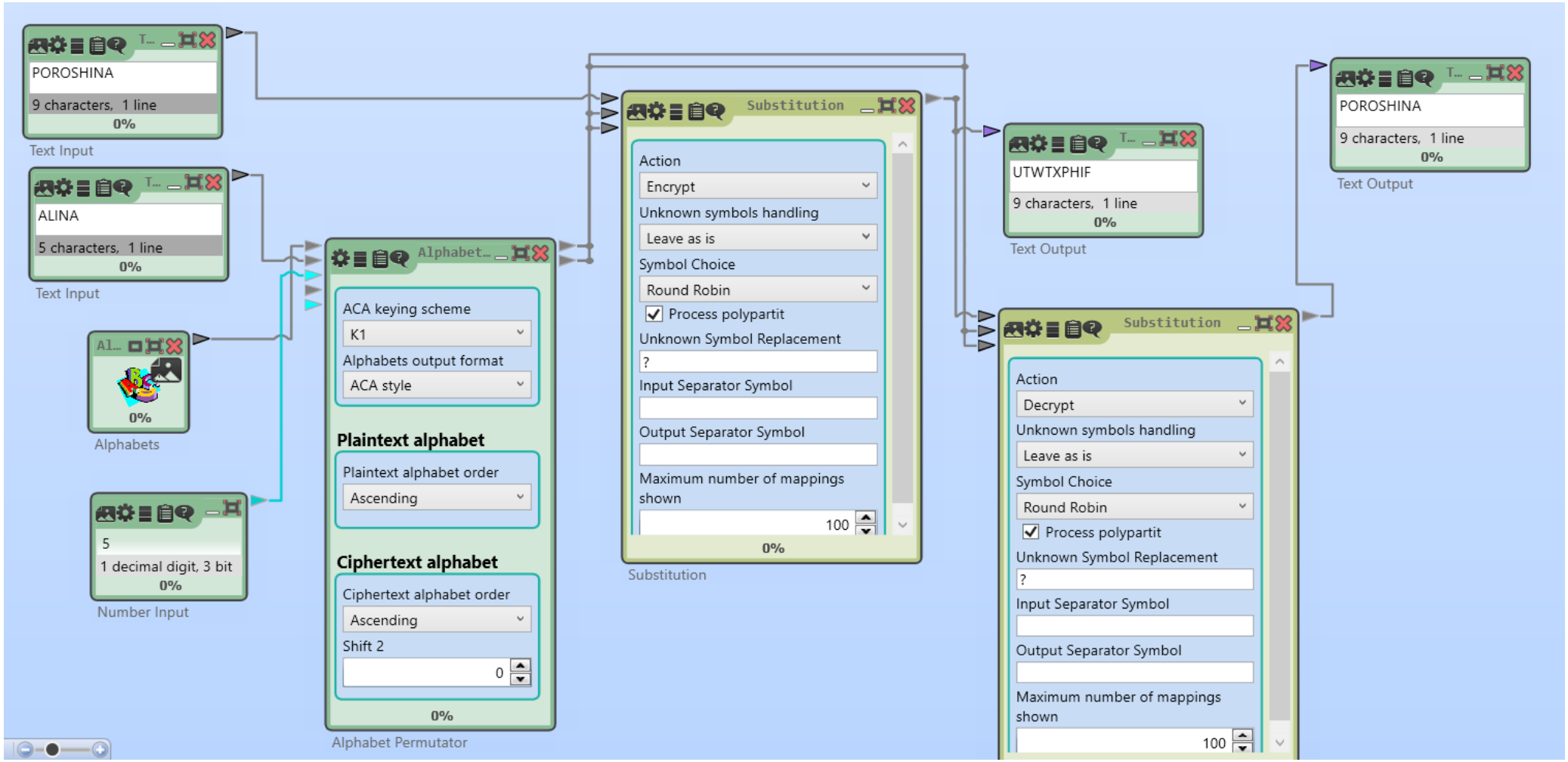
6. Повторить шифрование и атаку для тестов примерно в 300 и 150 символов.

7. Изучить возможности CrypTool 1 для автоматизации выполнения ручного расшифрования для текстов размером менее 300 символов.

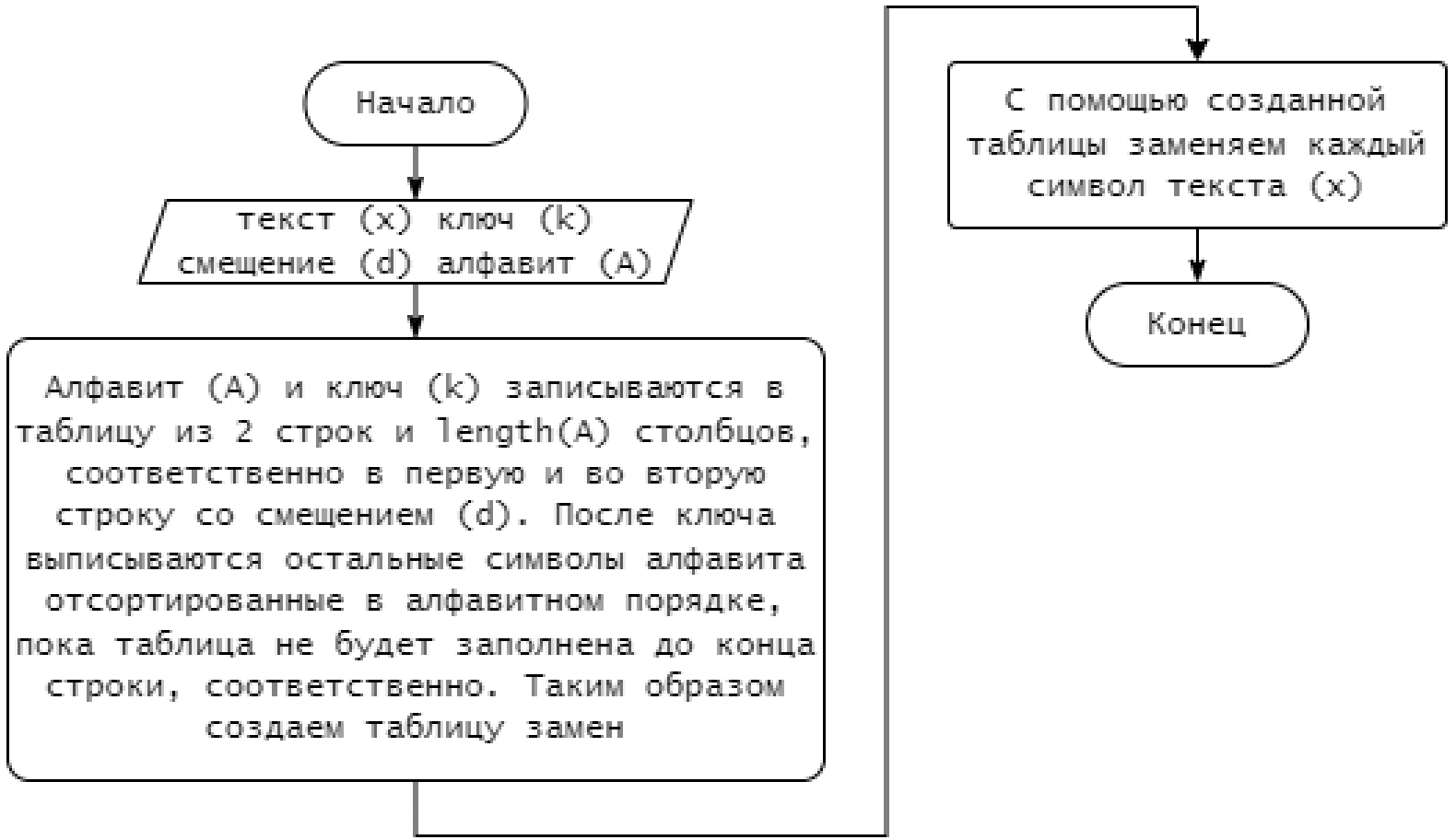
8. Выбрать новый абзац (примерно 600 символов) из файла English.txt (папка CrypTool/reference) и зашифровать его.

9. Дешифровать этот абзац, используя приложение Analysis –> Tools for Analysis и Analysis –> Symmetric Encryption(classic) –> Manual Analysis.

Реализация в CrypTool 2



Схема, поясняющая работу шифра



Заключение

1. Был изучен шифр «Моноалфавитной подстановки» и выявлены его следующие характеристики :

Шифр является шифром замены, где ключом служит пара ключевого слова и сдвиг.

При исследовании этого шифра, фамилия была зашифрована и расшифрована как вручную, так и с помощью CrypTool 2. Обе попытки привели к совпадающим результатам.

2. Была проведена атака методом "Frequency Analysis" с помощью программы CrypTool 2. По результатам атаки был составлен приближенный алфавит, из которого был выбран правильный.

3. Была проведена оценка сложности атаки «BruteForce», здесь A – мощность алфавита:

Оценка – $O(A!)$

Шифр двойной перестановки

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.

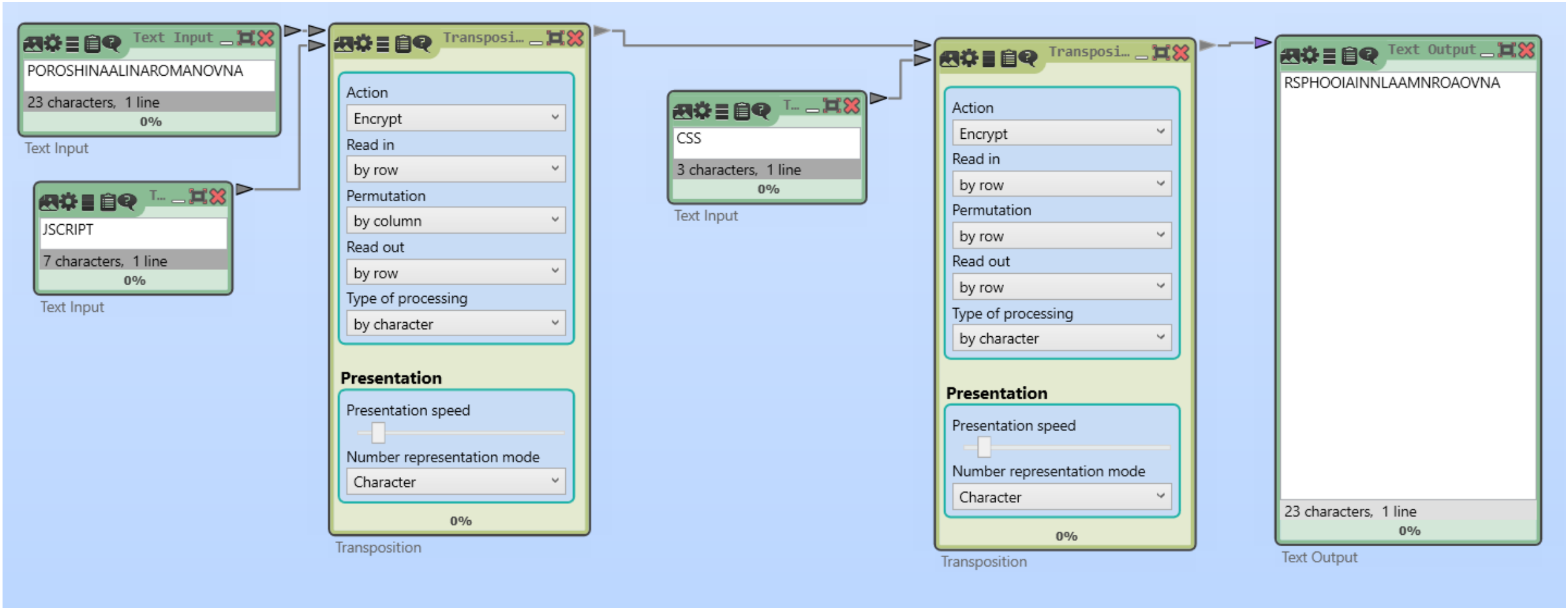
4. Зашифровать текст, содержащий ФамилиюИмяОтчество, и провести атаку, основанную на знании исходного текста, Analysis –> Symmetric Encryption(classic) –> Known Plaintext.

5. Выполнить самостоятельную работу:

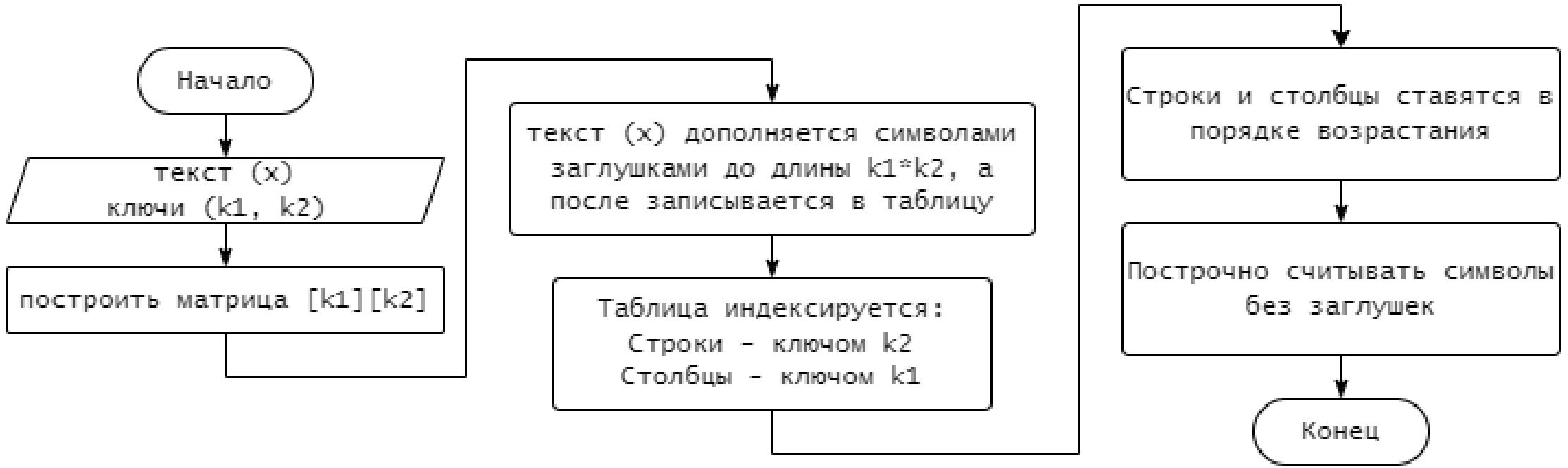
а) зашифровать текст с произвольным сообщением в формате «DEAR message THANKS», используя только одинарную перестановку. Обменяться подобными шифровками с коллегой по учебной группе для дешифровки при условии, что формы обращения и завершения письма известны;

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

Реализация в CrypTool 2



Схема, поясняющая работу шифра



Заключение

1. Был изучен шифр «Двойной перестановки» и выявлены его следующие характеристики:

Шифр использует перестановку, где два ключевых слова выступают в качестве ключа.

В ходе исследования этого шифра ФИО было зашифровано и затем успешно расшифровано как вручную, так и при помощи программы CrypTool 2, при этом результаты совпали.

2. Была проведена атака на шифр по известному тексту с помощью CrypTool 2 был получен верный ключ.

3. Была проведена оценка сложности атаки «BruteForce», здесь L – длина шифротекста:

Оценка – $O\ (L!)$

Шифр Виженера

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;

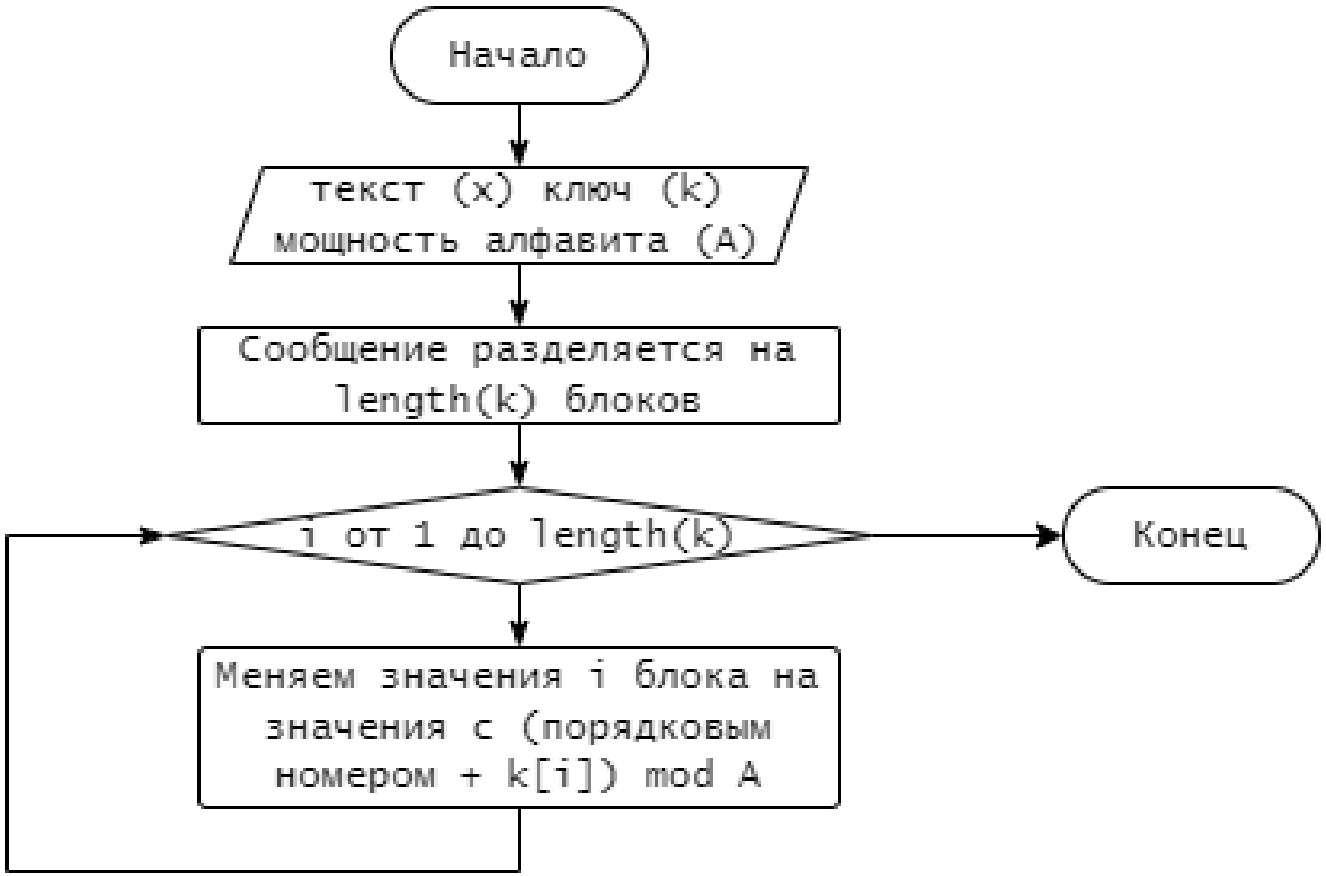
б) выполнить перестановку текста с размером столбца, равным размеру ключа, приложением Permutation/Transposition;

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.

Реализация в CrypTool 2

Схема, поясняющая работу шифра



Заключение

1. Был изучен шифр «Виженера» и выявлены его следующие характеристики :

Шифр использует блочную замену, где в качестве ключа выступает пара слов.

При исследовании этого шифра фамилия была зашифрована и успешно расшифрована как вручную, так и с применением программы CrypTool 2, и в обоих случаях полученные результаты совпали.

2. Была проведена атака методом "Frequency Analysis" с использованием программы CrypTool 2 на тексте, содержащем 2000 символов. В результате атаки был обнаружен правильный ключ.

3. Была проведена оценка сложности атаки «BruteForce», здесь L_A – длина алфавита:

Оценка – $O(L_A)$

Шифр Хилла

Задание

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

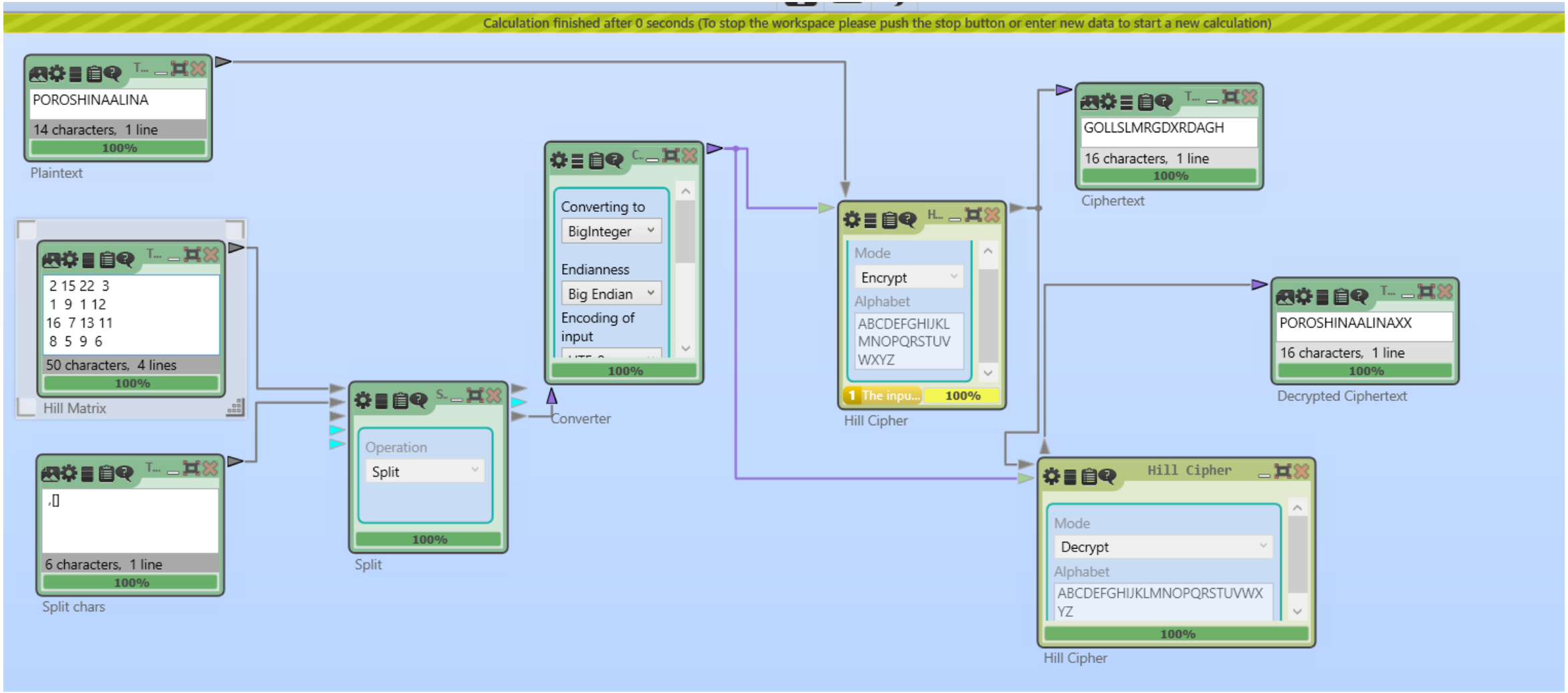
2. Зашифровать и расшифровать текст, содержащий только вашу фамилию (транслитерация латиницей), вручную и с помощью шифра с выбранным ключом 2 × 2. Убедиться в совпадении результатов. Проверить обратимость шифрующей матрицы (ключа).

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.

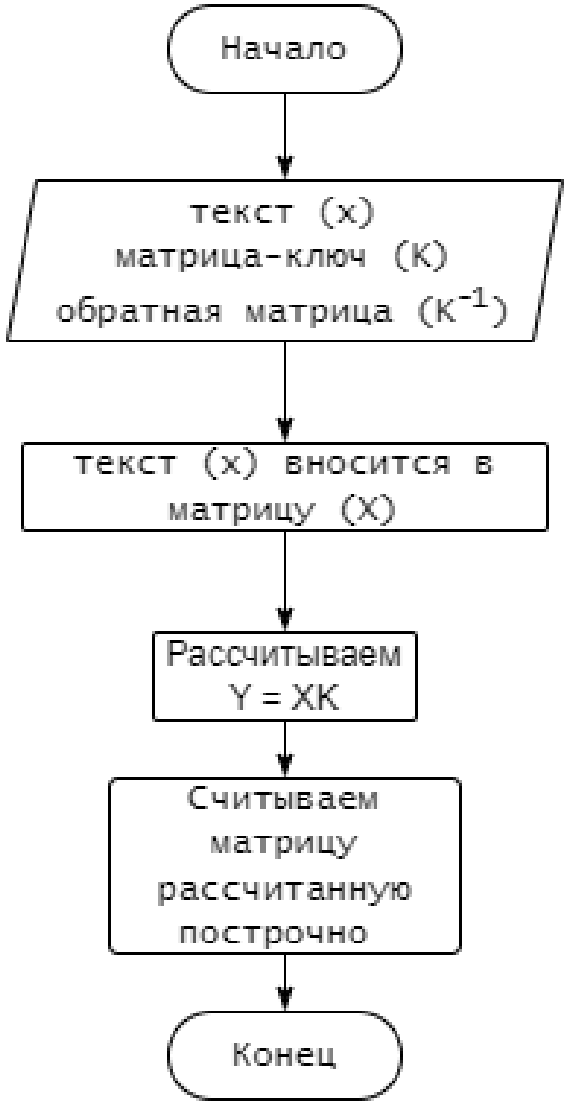
4. Выполнить атаку на основе знания открытого текста, используя приложение из Analysis –> Symmetric Encryption(classic) –> Known Plaintext.

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.

Реализация в CrypTool 2



Схема, поясняющая работу шифра



Заключение

1. Был изучен шифр «Хилла» и выявлены его следующие характеристики :

Шифр использует замену, где ключом является обратимая матрица.

В процессе исследования этого шифра текст был зашифрован и успешно расшифрован как вручную, так и с помощью программы CrypTool 2, и результаты совпали.

2. Была проведена атака методами в программе CrypTool 1. Был получен верный ключ.

3. Была проведена оценка сложности атаки «BruteForce», где $k \times k$ – размерность матрицы-ключа:

Оценка – $O\left(k^2\right)$

Комбинированный 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.

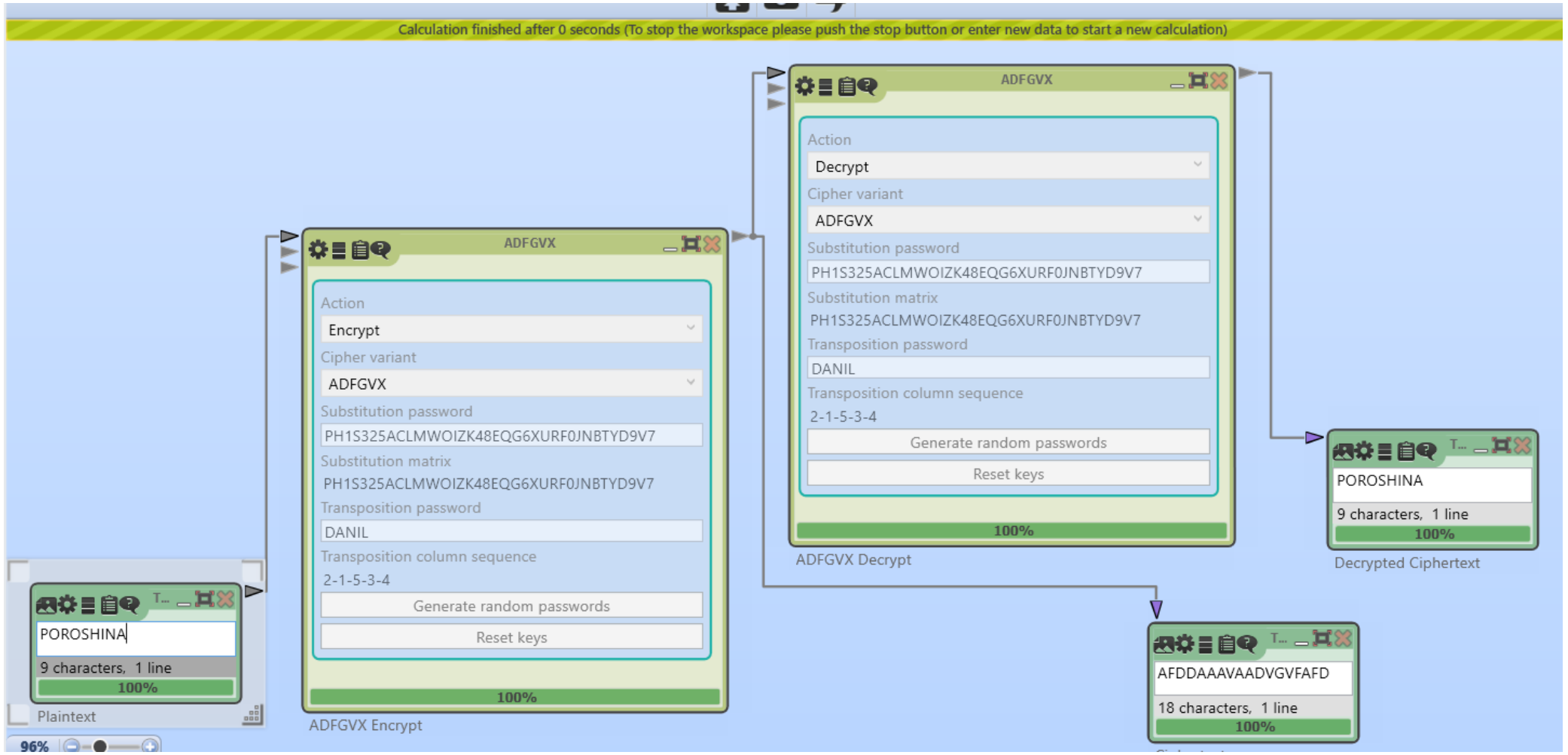
6. Изучить инструмент автоматизации ручного расшифрования для текстов менее 300 символов.

7. Выполнить самостоятельную работу:

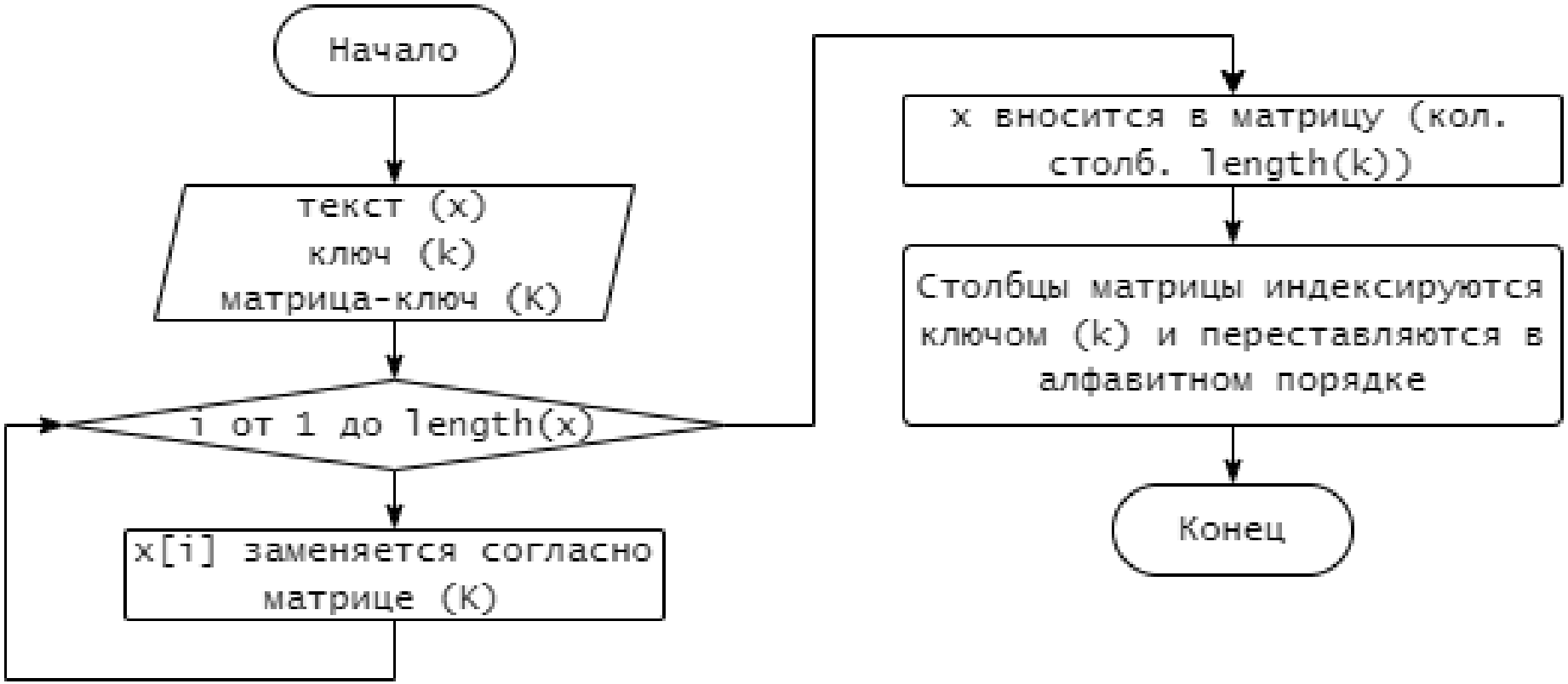
а) зашифровать текст из 200 символов, сохранить ключ, и обменяться шифровками с коллегой по группе для дешифровки;

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

Реализация в CrypTool 2



Схема, поясняющая работу шифра



Заключение

1. Был изучен комбинированный шифр «ADFGVX» и выявлены его следующие характеристики:

При анализе шифра было установлено, что он представляет собой комбинированный шифр, который использует как ключ матрицу и слово.

В ходе исследования этого шифра фамилия была зашифрована и успешно расшифрована как вручную, так и с помощью CrypTool 2, результаты совпали.

2. Была проведена атака методом перебора по словарю с помощью CrypTool 2, и верный ключ был найден спустя 14 минут и 40 секунды.

3. Была проведена оценка сложности атаки «BruteForce», где L – длина шифротекста:

Оценка – $O(L)$