**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Основы кибербезопасности»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

«**Анализ исторических шифров с помощью программного средства Cryptool 2**»

**Выполнил:**

студент группы M3206

Величко Максим Иванович



*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Таранов Сергей Владимирович

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Санкт-Петербург

2022 г.

***Цель***: с помощью программы CrypTool 2 изучить принципы работы исторических шифров, а также провести их криптоанализ.

***Ход работы***

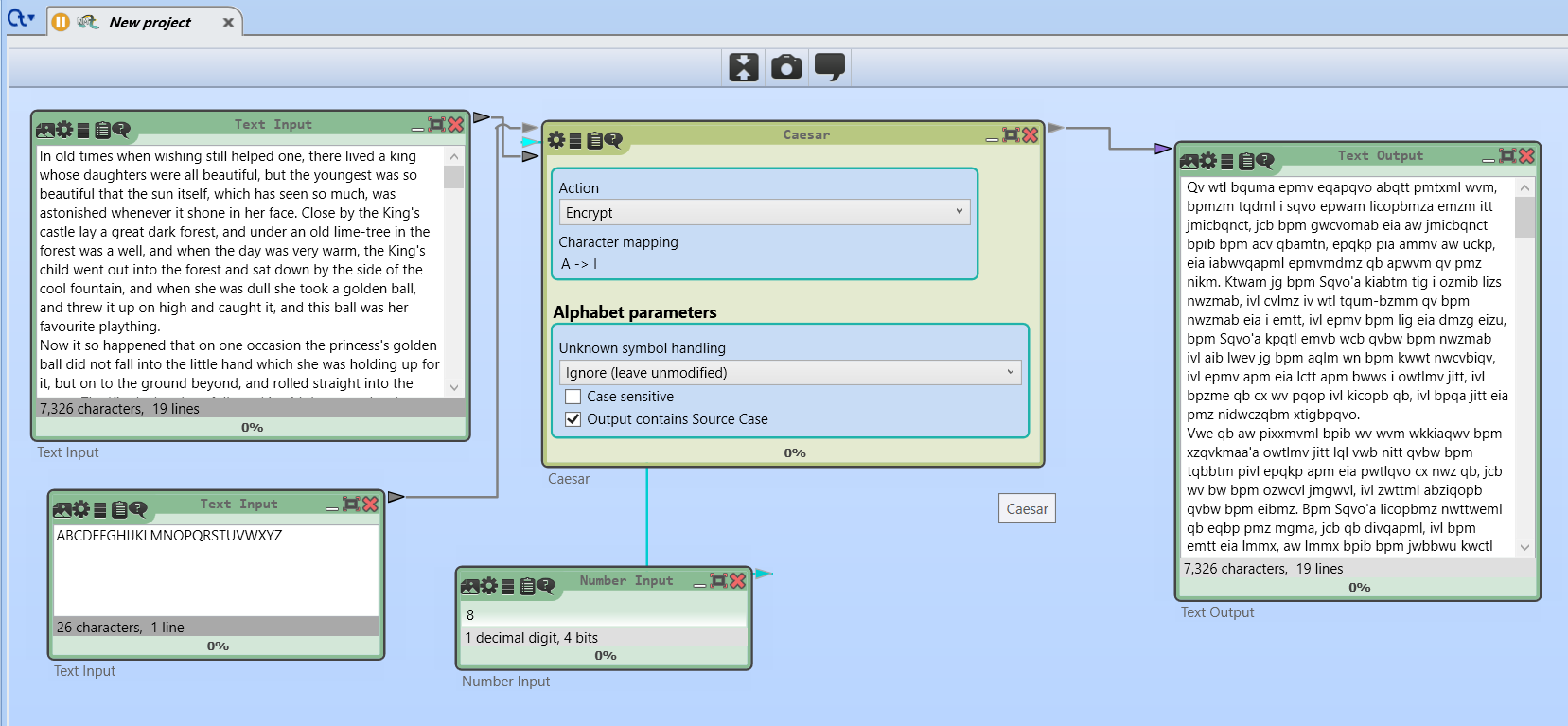
1. Необходимо зашифровать исходный текст с помощью шифра Цезаря.

Чтобы это реализовать необходимо перейти в Templates -> Cryptography -> Classical и

выбрать: Caesar Cipher. В поле - Text Input необходимо вставить открытый текст (я

выбрал английскую сказку объемом 7326 символов), затем выбрать действие

Encrypt и выбрать по какому ключу необходимо провести шифрование. В поле

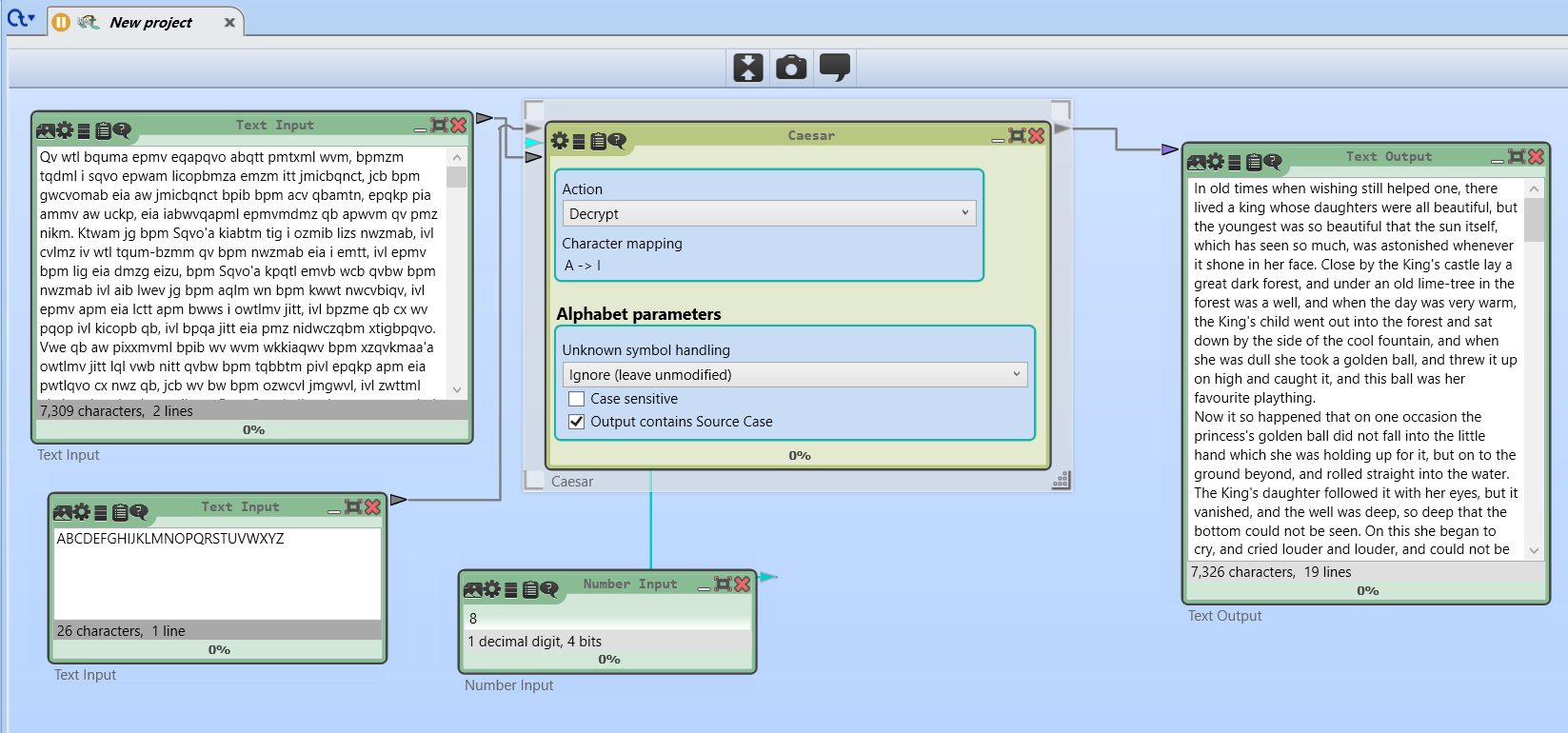
“Text Output” появится шифр текста.

2. Чтобы расшифровать полученный шифр текста необходимо использовать тот же

шаблон, в “Text Input” поместить шифр текст, выбрать действие Decrypt и

установить тот же ключ, который использовался при шифровании. В “Text Output”

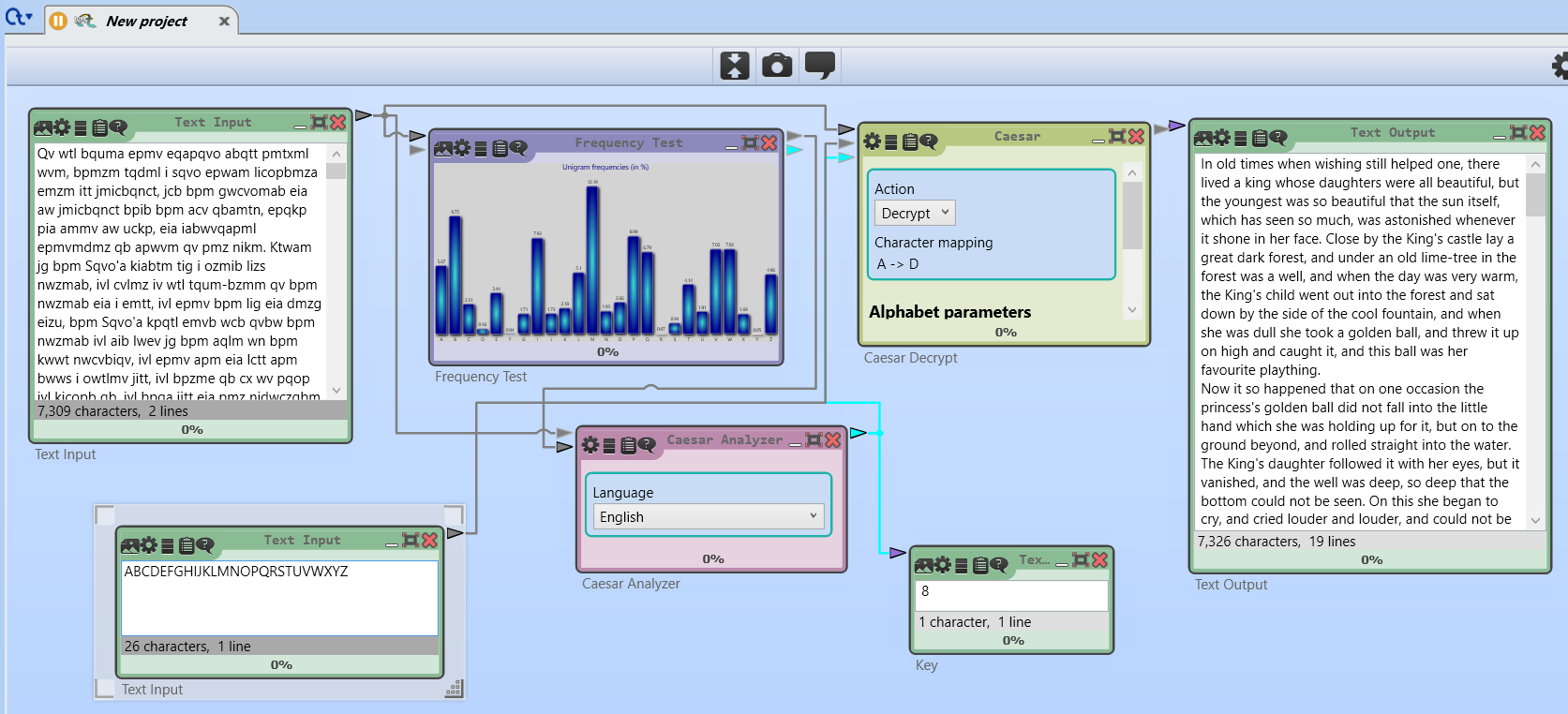
появится исходный текст.



3. CrypTool 2 позволяет расшифровать шифр Цезаря при помощи частного анализа.

Caesar Analyzer позволяет найти подобрать ключ, который использовался при

шифровании и дешифровать шифр текст.



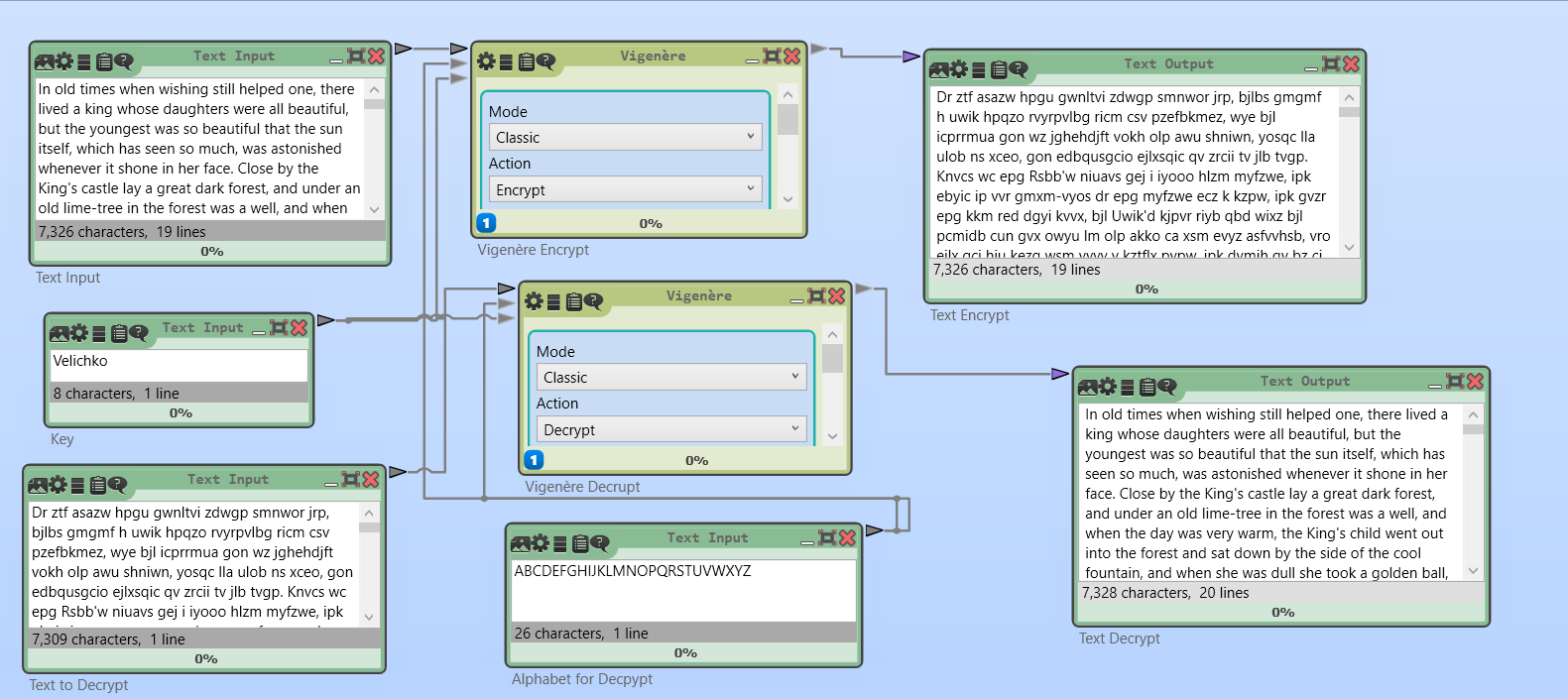
4. Необходимо зашифровать открытый текст с помощью шифра Виженера. В той же

вкладке Templates -> Cryptography -> Classical надо выбрать “Vigenère Cipher”. В “Text

Input” поместить тот же открытый текст и придумать ключ (я использовал свою

фамилию). После запуска в первой окне “Text Output” появится шифр текст, а во

втором окне исходный дешифрованный текст.



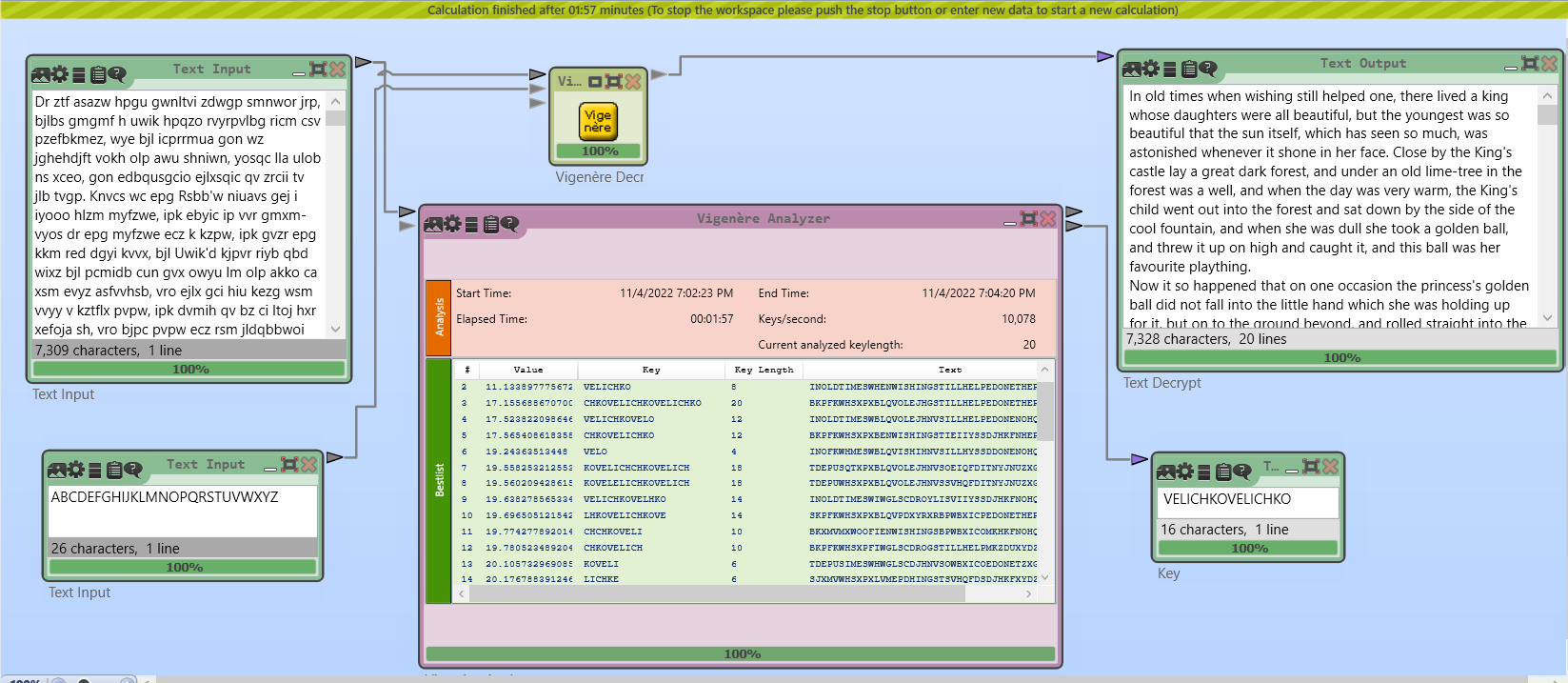
5. При проведении криптоанализа для шифра Виженера необходимо выбрать

соответствующий шаблон, в поле “Text Input” поместить шифр текст, запустить и

подождать некоторое время. Затем в поле “Text Output” появится расшифрованный

текст и в центральном блоке подобранный программой ключ, который

использовался при шифровании.

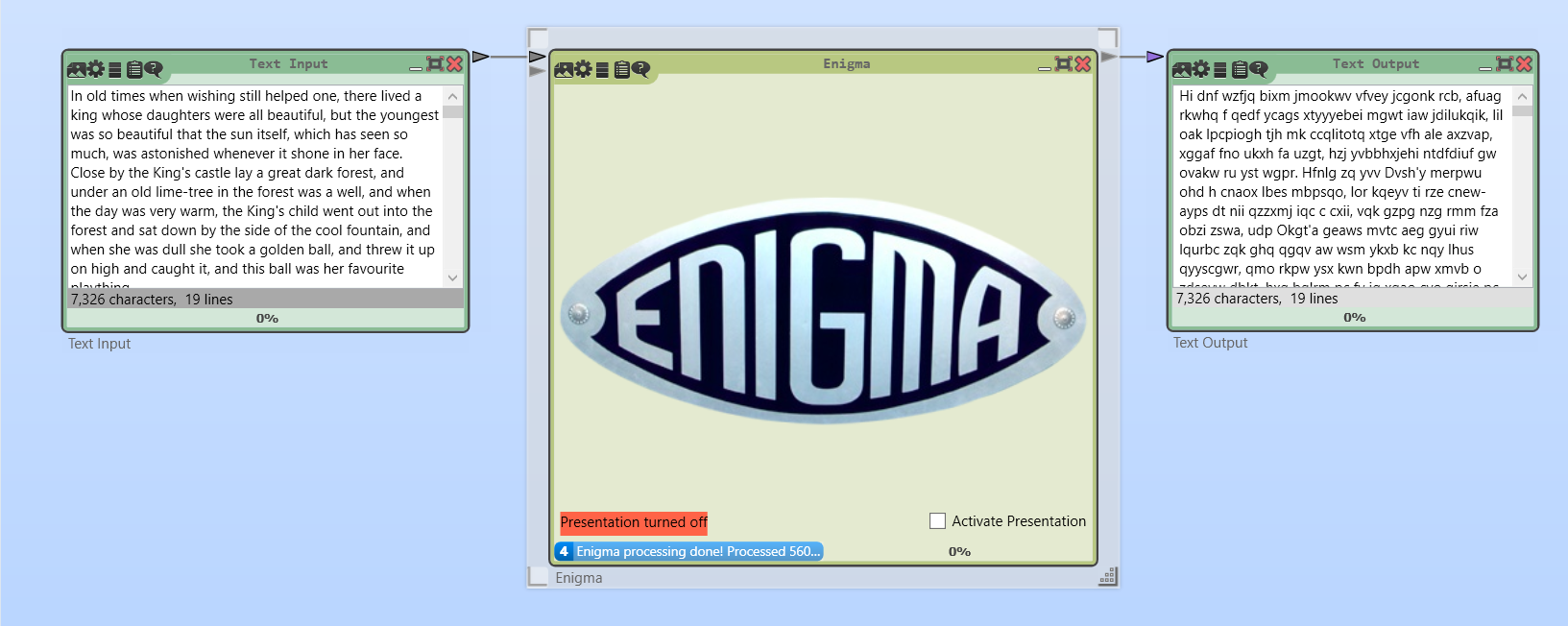


6. Для шифрования открытого текста при помощи Enigma Machine необходимо

выбрать соответствующий шаблон и поместить в “Text Input” все тот же исходный

текст. В параметрах можно настроить то, как будет проводиться шифрование.

После старта в “Text Output” появится закрытый текст.



7. Для дешифрования необходимо шифр текст поместить в поле, куда изначально

помещался исходный текст и настроить параметры так же, как при шифровании.

Таким образом мы получим дешифрованный текст.

Изображение выглядит как текст

Автоматически созданное описание

8. При проведении криптоанализа зашифрованного текста машиной Enigma

необходимо выбрать соответствующий шаблон и поместить в “Text Input”

шифр текст и запустить работу. Спустя некоторое время в “Text Output” появится

расшифрованный текст, а в центральном блоке появится ключ, который

использовался для шифрования. Также будет выведена диаграмма частоты

встречаемости букв.

Изображение выглядит как текст

Автоматически созданное описание

***Вывод***: в ходе выполнения лабораторной работы я познакомился с программой CrypTool и ее возможностями. Произведено шифрование и дешифрование открытого текста историческими шифрами: шифром Цезаря, шифром Виженера и машиной Enigma. Также был проведен криптоанализ каждого шифра, по результатам выполнения которого можно утверждать, что шифр Цезаря имеет наименьшую криптостойкость среди остальных шифров, а шифр, полученный при использовании машины Enigma является наиболее криптостойким, поскольку на его анализ и дешифрование приходится больше всего времени.