**1. Анализ исторических шифров с помощью программного средства Cryptool 2.**

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

**Задачи практической работы**

Используя функции программы CrypTool 2, проанализировать следующие криптографические примитивы:

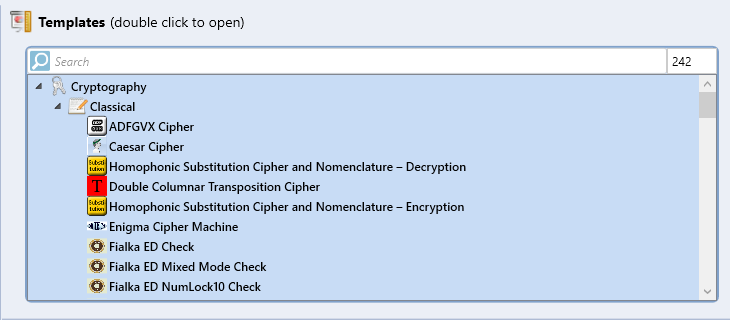
1. Шифр Цезаря, шифры перестановки и замены (как примеры моноалфавитных шифров);
2. Шифр Виженера (как пример полиалфавитного шифра);
3. Структуру и процесс шифрования в роторной машине Энигма.

Изучение каждого криптографического алгоритма предлагается проводить по следующему плану исследования:

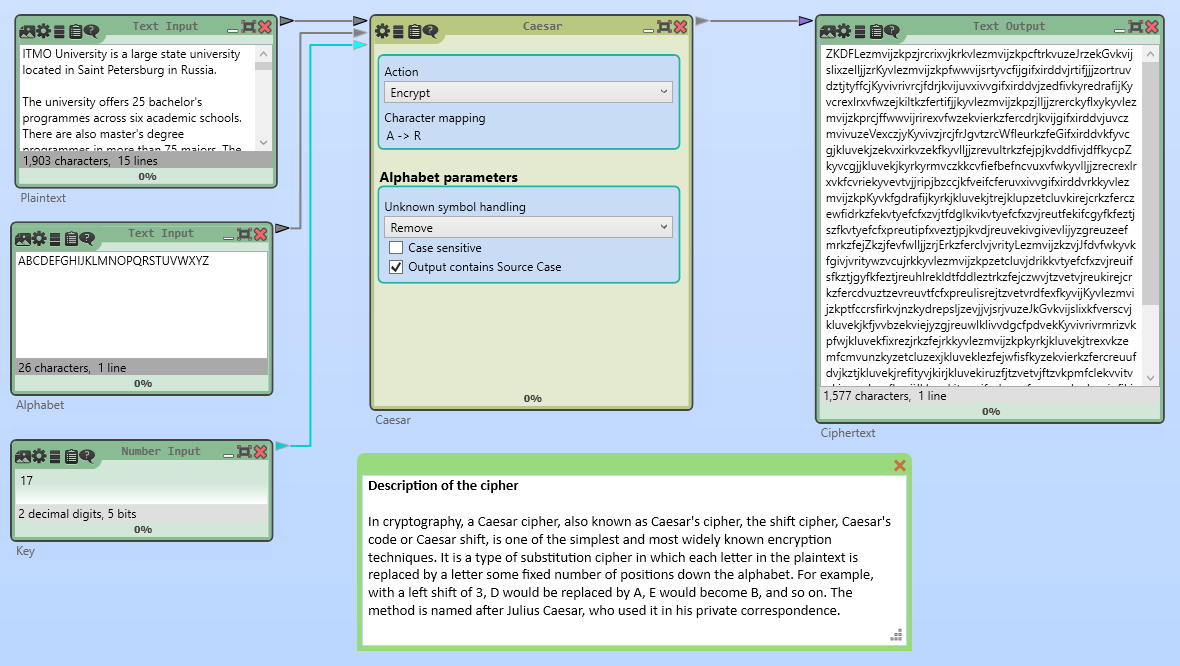
1. Выполнить шифрование своего примера открытого текста с собственными настройками криптосистемы. Получить шифротекст, соответствующий заданному входному значению и ключу. Изучить настройки криптосистемы, а именно: возможное пространство ключей, дополнительные механизмы для шифрования и повышения криптостойкости, ограничения и требования к параметрам криптоалгоритма (ограничения на длину криптографического ключа, алфавит открытого текста и шифротекста, слабые параметры, обязательные и рекомендуемые требования к настройке криптосистемы).
2. Выполнить дешифрование закрытого текста с помощью криптографического ключа из первого пункта плана. Оценить, насколько сложно выполнить атаку на ключ методом перебора. Проанализировать сложность процесса шифрования и настройки криптосистемы для использования (шифрования/дешифрования).
3. Выполнить простейший криптоанализ, используя шаблоны из программы Cryptool 2. При криптоанализе можно использовать шифротекст или несколько шифротекстов, полученных на первом пункте плана исследования. При криптоанализе считается, что криптографический ключ неизвестен, более того, что нет никакой коррелирующей информации о ключе. Шифротексты без криптографических ключей можно получить на этапе шифрования криптосистемы в Cryptool 2, скрыв предварительно поле для ввода ключа.

**Порядок выполнения работы.**

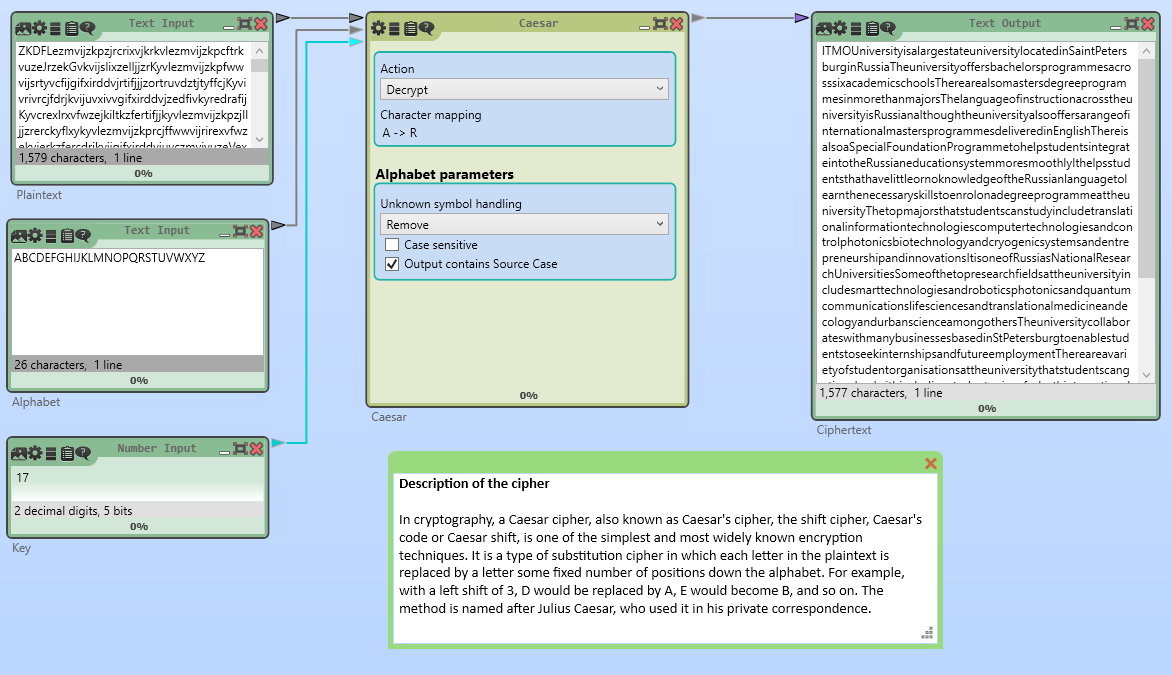
1. Выполните шифрование открытого текста, основываясь на примере криптосистемы, реализованной в программном средстве СrypTool 2. Для того чтобы открыть соответствующий шаблон в программном средстве перейдите в Раздел Templates в подкаталог Cryptography -> Classical -> Caesar Chipher



1. Откройте шаблон для шифрования с помощью шифра Цезаря. Задайте собственный открытый текст в поле Plaintext, разрешенный алфавит в поле Alphabet и значение криптографического ключа. Открытый текст и ключ выбирается самостоятельно. Для более быстрого и успешного последующего криптоанализа необходимо, чтобы открытый текст был как можно больше, не желательно, чтобы он содержал недопустимых шифром значений (знаков пунктуации, скобок, вставок из другого алфавита и пр.) Сохраните получившийся шифротекст из поля Ciphertext и значение ключа для дальнейшего использования.

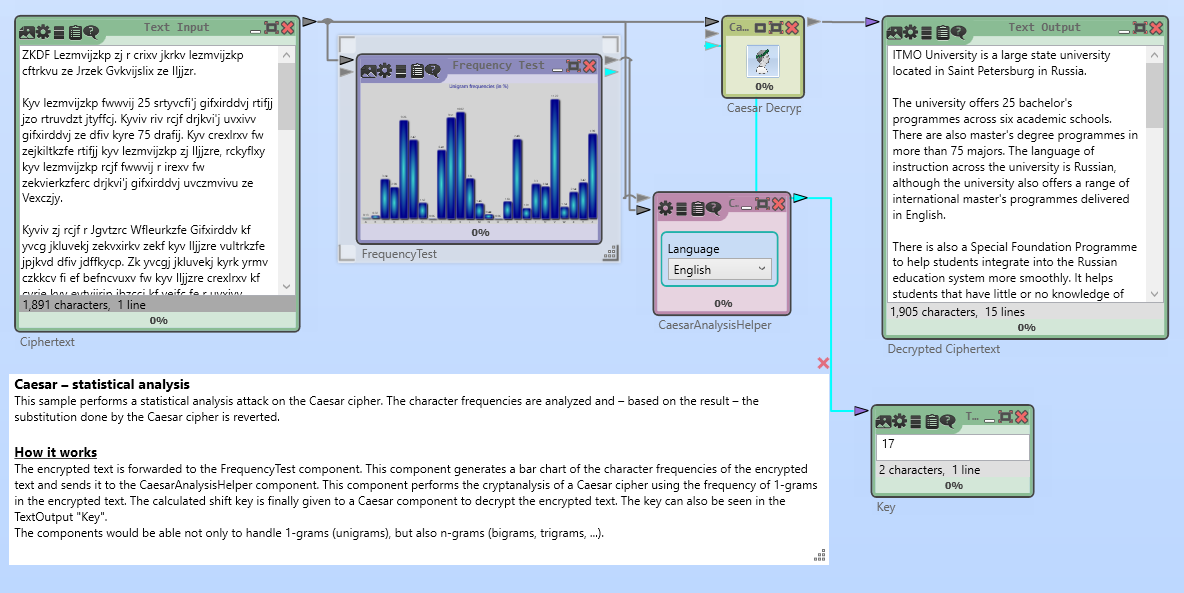


1. Выполните дешифрование с помощью того же шаблона, выбрав в блоке Caesar режим дешифрования. Проанализируйте выходное значение. Совпадает ли оно полностью с открытым текстом из пункта 2?



1. Выполнить простейший криптоанализ, используя шаблоны из программы Cryptool 2 (шаблон для атаки на основе частотного анализа находятся по пути Templates -> Cryptoanalysis -> Classical -> Caesar Analysis using character frequencies). Целью криптоанализа является восстановление секретного ключа на основе закрытого текста. В качестве входных параметров предлагается указать закрытый текст, который был получен в пункте 2 и попытаться восстановить открытый текст и секретный ключ. Проанализируйте путем шифрования других шифротекстов и с помощью частотных характеристик то, как влияет на успешность криптоанализа следующие критерии:

* Длина открытого текста;
* Удаление специальных символов и вставок, которые не входят в алфавит шифра (формул, ковычек, обозначений переменных и пр.);
* Удаление пробелов между словами.



1. Выполните криптоанализ шифра Цезарь, используя шаблон, реализующий атаку полным перебором. Путь до шаблона Templates -> Cryptoanalysis -> Classical -> Caesar Brute Force Analysis.
2. По аналогии с пунктами 1-5 провести анализ других моноалфавитных и полиалфавитных шифров из практической работы, а также провести атаки на каждый криптоалгоритм. Необходимые шаблоны Cryptool 2 (Templates -> Cryptoanalysis/Cryptography -> Classical):

для шифров:

* Substitution Cipher;
* Transposition Cipher;
* Vigenère Cipher.

для атак на шифры:

* Transposition Brute-Force Analysis;
* Transposition Crib Analysis;
* Transposition Genetic Analysis;
* Transposition Hill Climbing Analysis;
* Monoalphabetic Substitution Analyzer;
* Frequency Analysis;
* Vigenère Analysis.

1. Выполните пункты 1-5 для эмулятора роторной машины Энигмы. Необходимые шаблоны Cryptool 2 (Templates -> Cryptoanalysis/Cryptography -> Classical):

для Энигмы:

* Enigma Cipher Machine.

для атак на роторную машину Энигма:

* Enigma Gillogly Attack;
* Enigma Hillclimbing Attack;
* Enigma Simulated Annealing Attack;
* Enigma Turing Bombe Attack.

Для взлома Энигмы разрешается уменьшить пространство ключей для перебора. Для этого можно в настройках блока для атаки уменьшить пространство ключей для перебора, например, можно перебирать только значения 1-2 роторов, а все остальные ключевые значения Энигмы (кольца, типы роторов и рефлектора, коммутационная панель) выставить на те значения, которые вы использовали на этапе шифрования.

**Альтернативный вариант** лабораторной предусматривает программную реализацию рассматриваемых в работе шифров (простые шифры сдвига, замены и перестановки, шифр Виженера, программная имитация работы роторной машины Энигмы). Необходимо реализовать все представленные шифры из списка. Каждый шифр из списка может быть заменен на другой шифр из того же класса, например, простой шифр замены можно заменить на моноалфавитный аффинный шифр, роторную машину Энигма на роторную машину M209, полиалфавитный шифр Виженера на полиалфавитный шифр Бофора и т.д. То есть моноалфавитный шифр на любой моноалфавитный, полиалфавитный на любой полиалфавитный, роторную машину на любую роторную машину. Если затрудняетесь сопоставить понравившийся шифр для изучения - можно уточнить у преподавателя.

**Вопросы для защиты**

1. Что изучают следующие разделы криптографии: криптология, криптография, криптоанализ?

2. Основные отличия, определения, примеры для следующих систем: асимметричные криптосистемы, симметричные криптосистемы, криптографические протоколы.

3. Выделите примеры шифров для каждого этапа развития криптографии: наивная криптография, формальная криптография, математическая криптография.

4. Шифры замены, перестановки и сдвига

5. Атака полного перебора ключа и частотный анализ символов

6. Модульная арифметика. Простые примеры.

7. Шифр Виженера. Тест Казисского

8. Принцип Кергоффса

9. Роторные машины. Краткое описание принципа работы и внутренней структуры. Пространство ключей роторной машины.

10. Криптостойкость. Вычислительная(практическая) и математическая(теоретическая) криптостойкость.

11. Примеры криптосистемы этапа математической криптографии.

12. Криптоанализ. Классический криптоанализ. SCA.

13. Свойство диффузии и конфузии. Их связь с элементарными операциями в шифрах (перестановка, замена, сдвиг)