Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Евсеева Дарья Олеговна

22 октября, 2022

Содержание

# Цель работы

Целью данной работы является освоение на практике применения режима однократного гаммирования.

# Задание

Разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# Теоретическое введение

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.

# Выполнение лабораторной работы

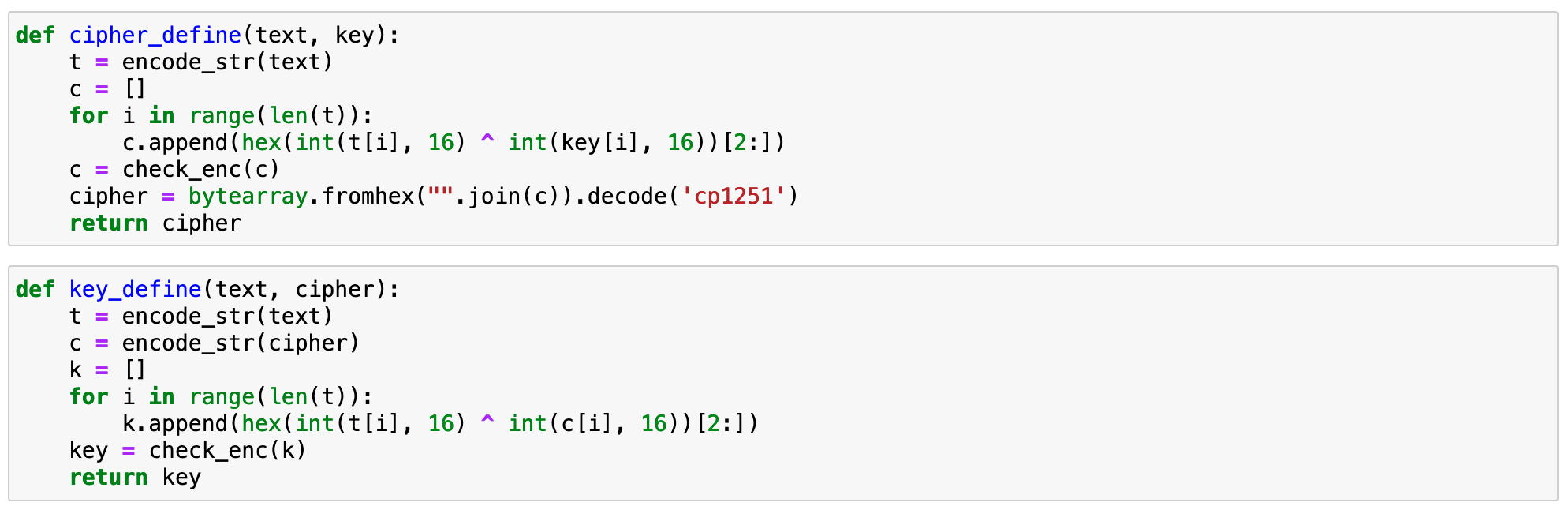
Выполнять работу будем в среде Jupyter Notebook на языке Python.

Для начала импортируем необходимую библиотеку и определим вспомогательные функции для дальнейшей работы.



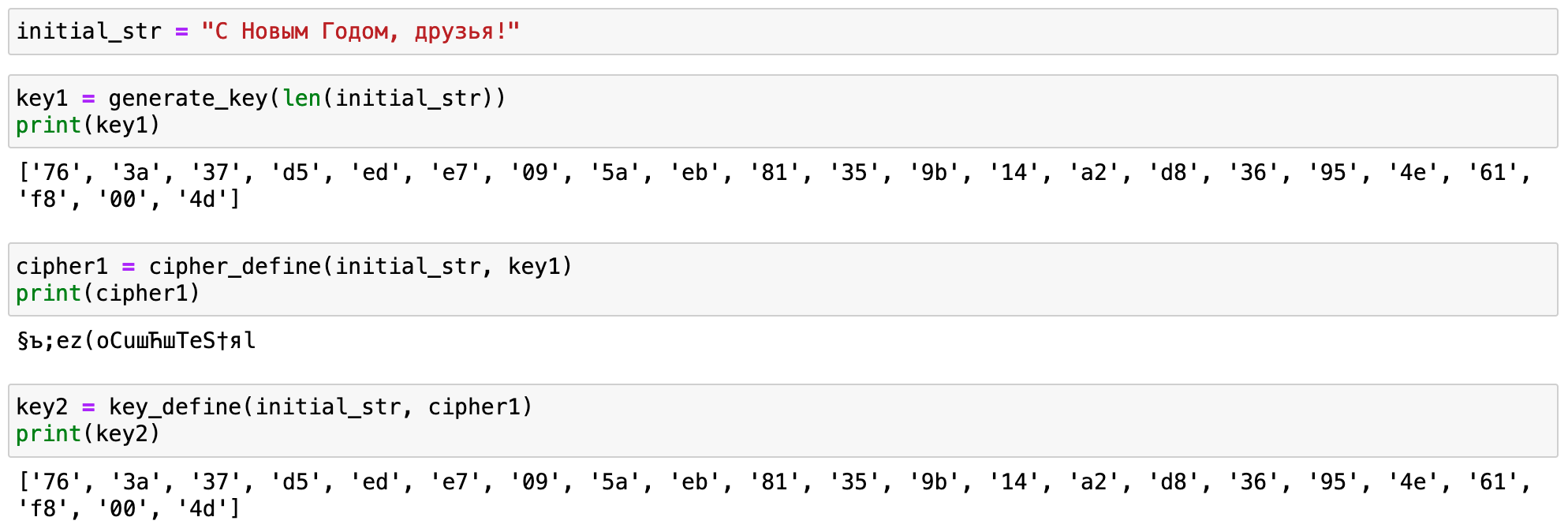
Вспомогательные функции

Далее определим основные функции. Функция cipher\_define будет использоваться для определения вида шифротекста при известном ключе и известном открытом тексте, а функция key\_define — для определения ключа, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой вариант прочтения открытого текста.



Основные функции

Далее проверим работу определенных ранее функций и убедимся в правильности результатов.



Проверка работы

Как мы видим, все функции успешно работают.

# Выводы

В результате проделанной работы мы освоили на практике применение режима однократного гаммирования.

# Список литературы

* Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН” https://esystem.rudn.ru/