Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Монастырская Кристина Владимировна

Содержание

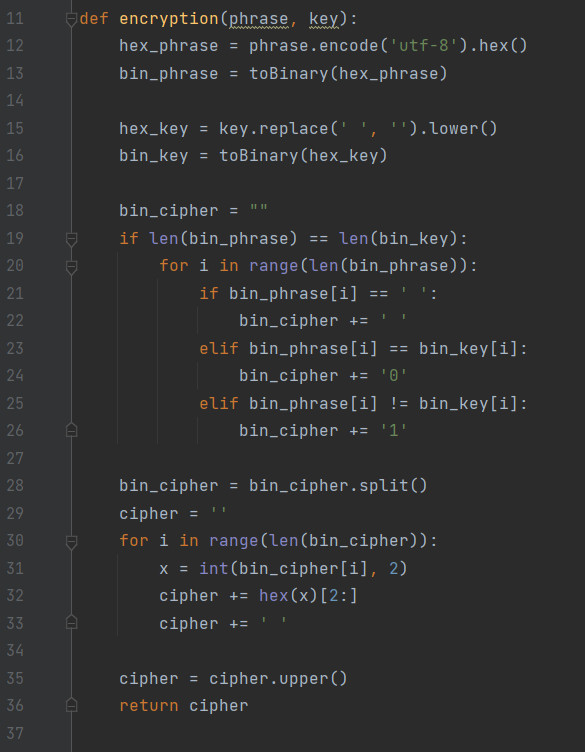
# Цель работы

Освоить на практике применение режима однократного гаммирования. [[1]](#список-литературы)

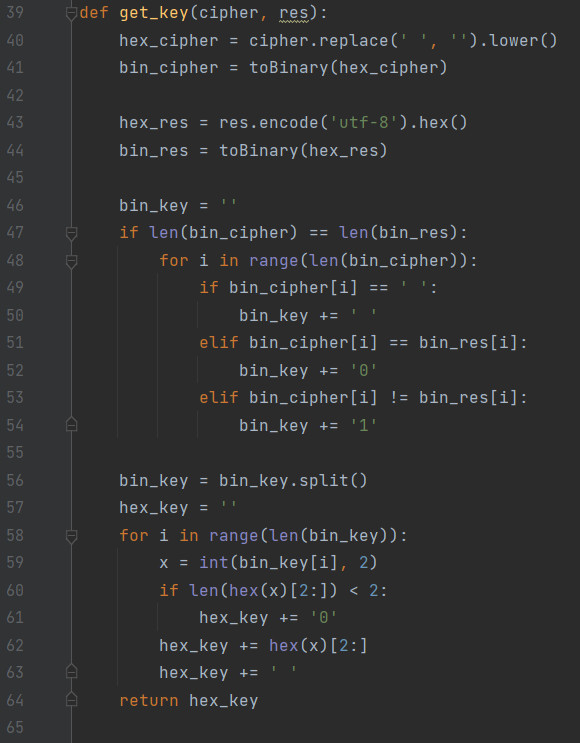
# Выполнение лабораторной работы

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

Приложение может: 1. Определять 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.

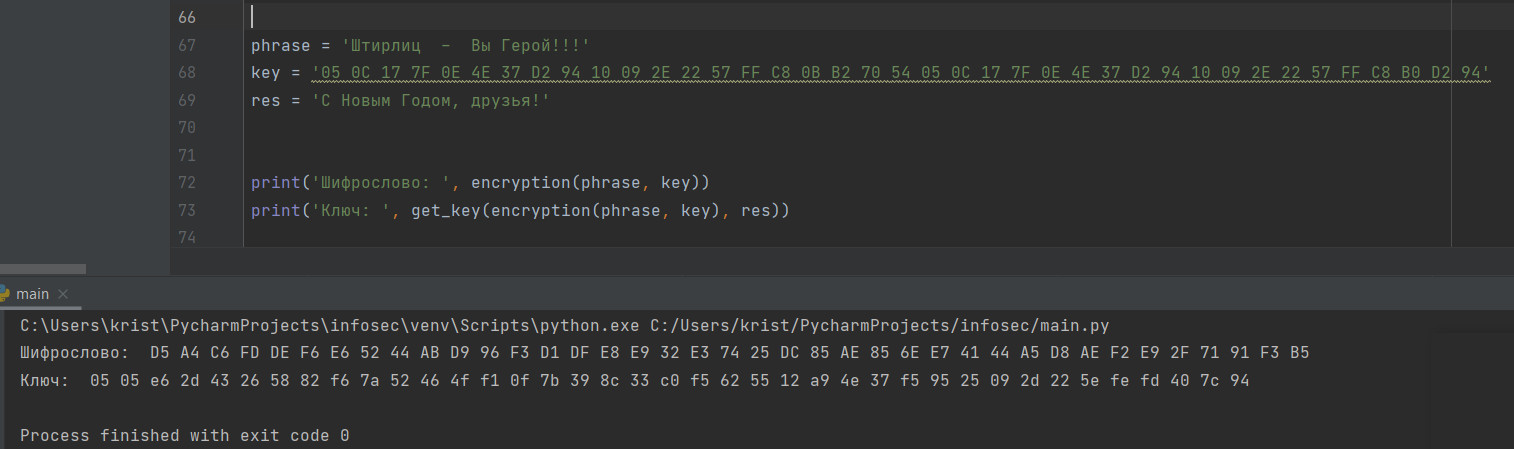
Для реализации первого пункта реализовала функцию encryption (([рис. 1](../images/1.jpg)) В данной функции реализовано преобразование исходного текста и ключа в двоичный код в виде строки, а далее с этими строками происходит сложение по модулю 2. Благодаря этим действиям мы получили шифротекст в двоичном коде, который мы преобразовали в шестнадцатиричную строку. 

Для реализации второго пункта реализовала функцию get\_key (([рис. 2](../images/2.jpg)), в которой нашла ключ преобразующий шифротекст в какой-либо заданный открытый текст. Функция реализована схожим образом: открытый итоговый текст и шифротекст преобразовываются в двоичный код, далее производится операция подбора значений ключа исходя из шифротекста и итогового текста. Получается аналогичное сложение по модулю 2. После этого ключ преобразуется в шестнадцатиричный формат.



Функция get\_key

Результат работы программы (([рис. 3](../images/4.jpg)):



Результат работы программы

# Выводы

Освоить на практике применение режима однократного гаммирования.

# Список литературы

1. [Основы безопасности информационных систем : Учеб. пособие для студентов вузов, обучающихся по специальностям “Компьютер. безопасность” и “Комплекс. обеспечение информ. безопасности автоматизир. систем” / Д.А. Зегжда, А.М. Ивашко. - М. : Горячая линия - Телеком, 2000. - 449, [2] с. : ил., табл.; 21 см.; ISBN 5-93517-018-3](https://search.rsl.ru/ru/record/01000682756).