Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Пономарева Лилия Михайловна

Содержание

# Цель работы

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

# Теоретическое введение

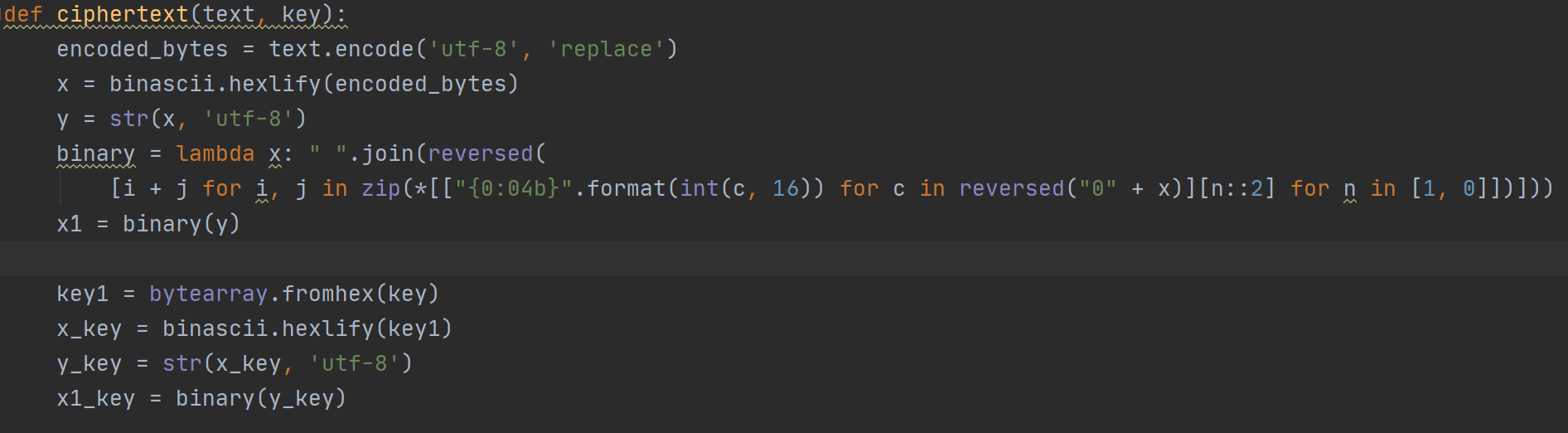
Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами 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. Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста. Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой. Открытый текст имеет символьный вид, а ключ — шестнадцатеричное представление. Ключ также можно представить в символьном виде, воспользовавшись таблицей ASCII-кодов.

# Выполнение лабораторной работы

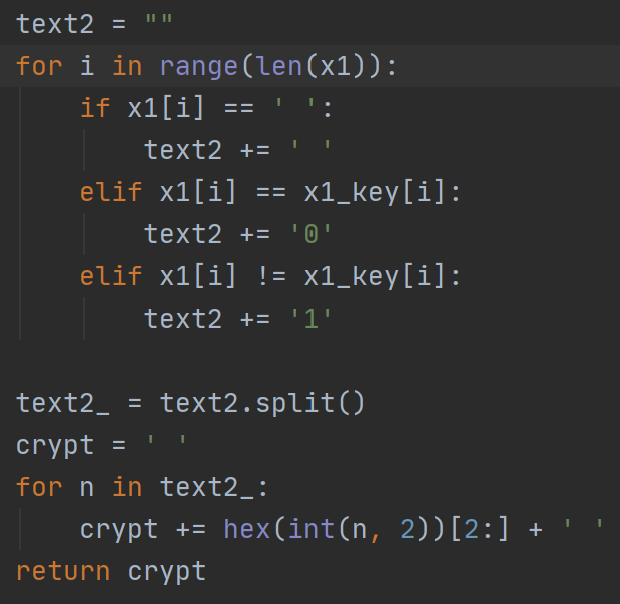
Разработала приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

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 ciphertext (([рис. 1](../../image/1.png)), в которой с помощью сложения по модулю 2 нашла шифротекст при известном ключе и открытом тексте(([рис. 2](../../image/2.png)).

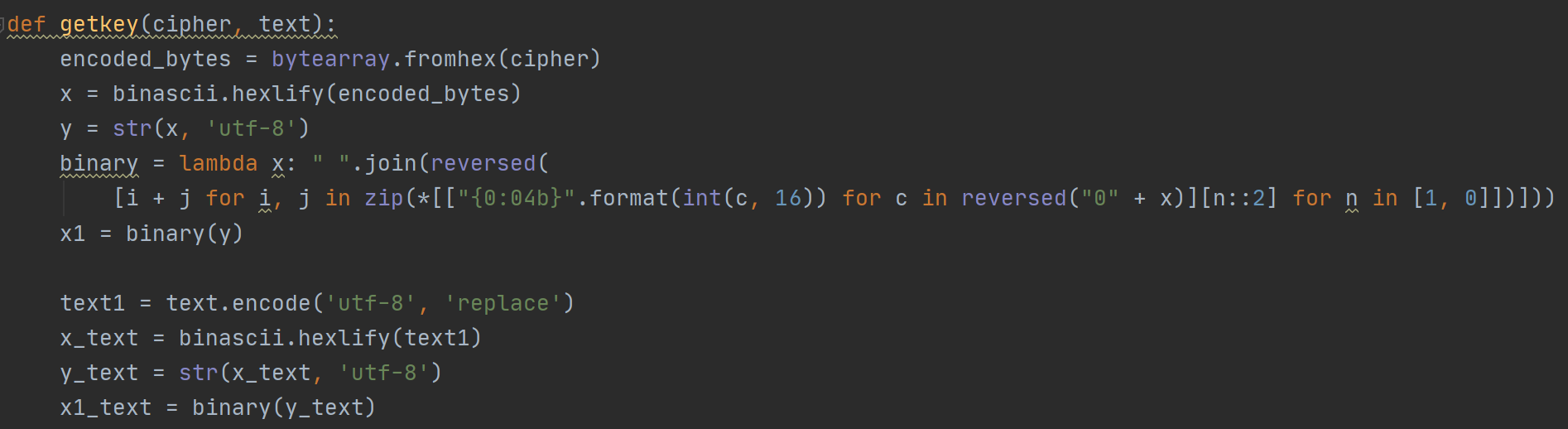


Представление данных в двоичном виде

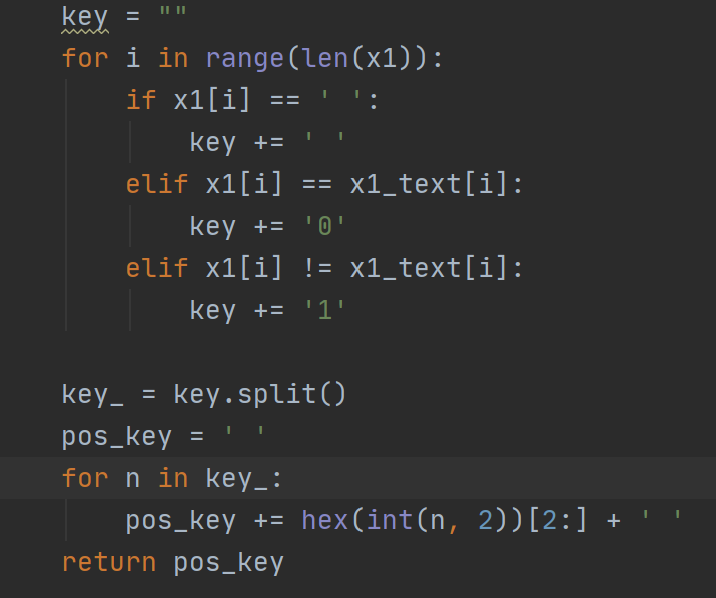


Реализация сложения по модулю

Для реализации второго пункта реализовала функцию getkey (([рис. 3](../../image/3.png)), в которой нашла ключ преобразующий шифротекст в какой-либо другой(([рис. 4](../../image/4.png)).

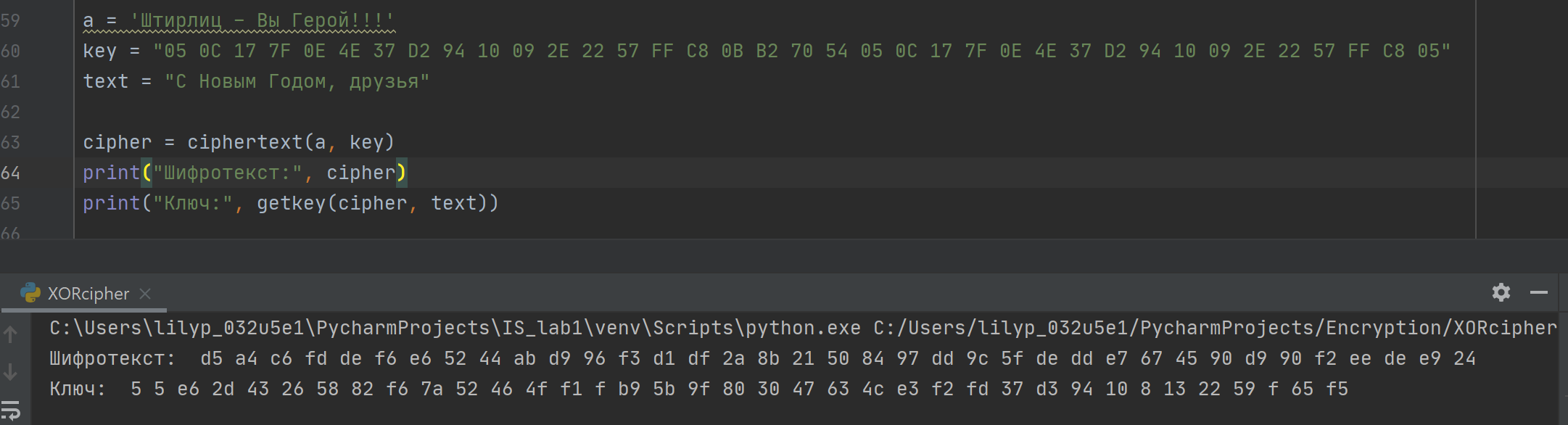


Представление данных в двоичном виде



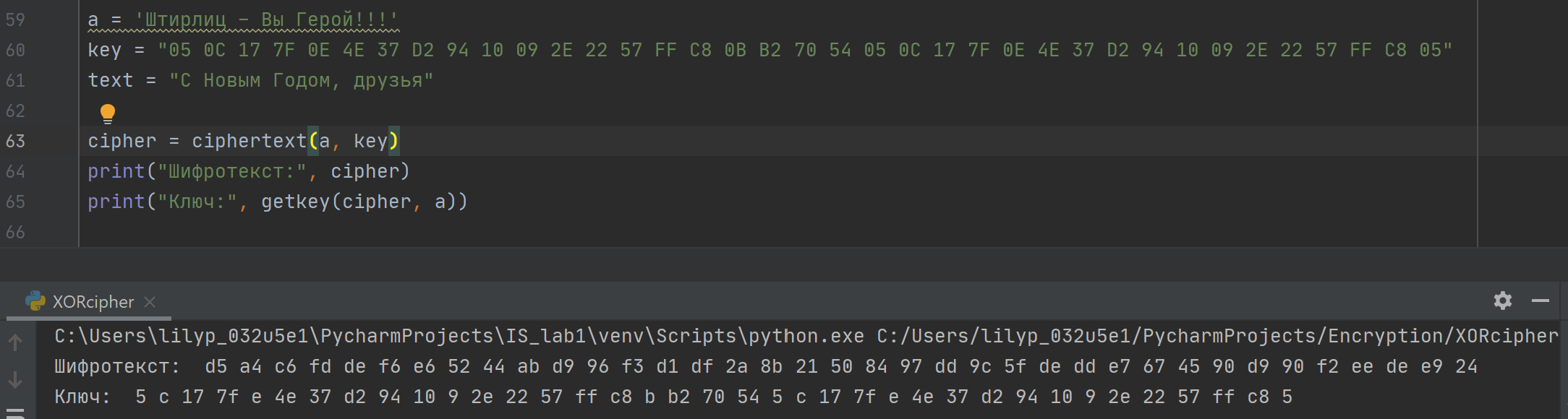
Получение ключа

Подобрала ключ, чтобы получить сообщение «С Новым Годом, друзья». (([рис. 5](../../image/5.png))



Ключ сообщения

Также произвела проверку работы функции getkey (([рис. 6](../../image/6.png))



Получение изначального ключа

# 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).