Отчет по лабораторной работе №8

Лабораторная работа №8: Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом.

Голова Варвара Алексеевна, НФИбд-03-18

2021, 18 December

Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Выполнение работы

## Алфавит

Задала алфавит из русских букв и алфавит из соответствующих им шестнадцетиричных чисел.



Figure 1: Алфавиты

## Сообщения

Ввела сообщения.

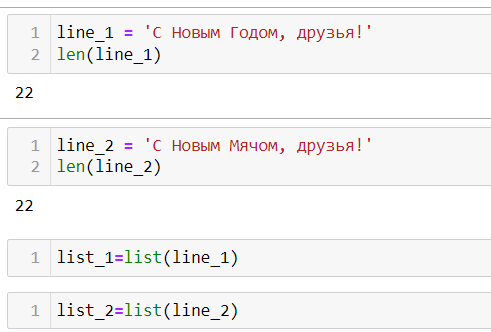


Figure 2: Сообщения

## Ключ

Создала рандомный ключ.

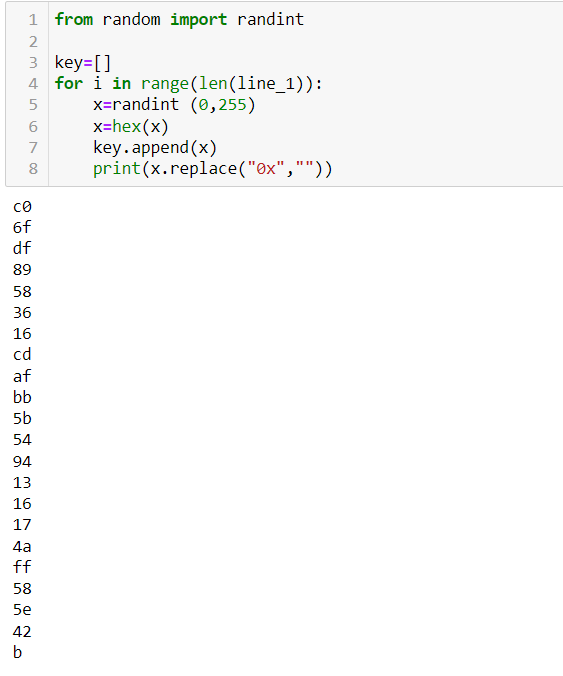


Figure 3: Создание ключа

## Перевод сообщений

Перевела заданные сообщение в шестнадцетиричные числа.

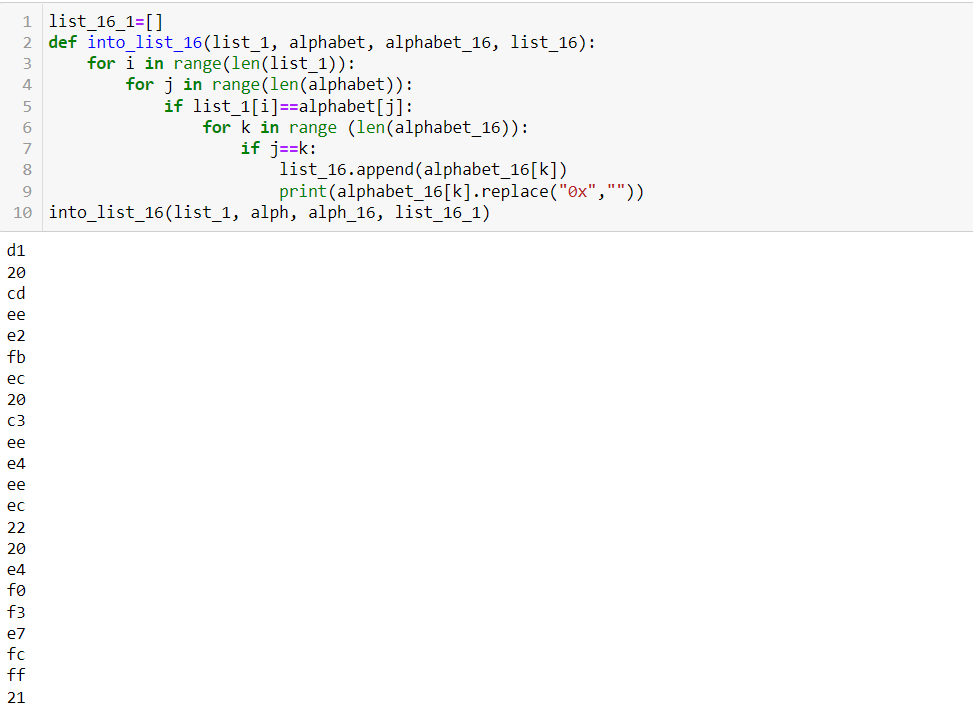


Figure 4: Шестнадцетиричная система

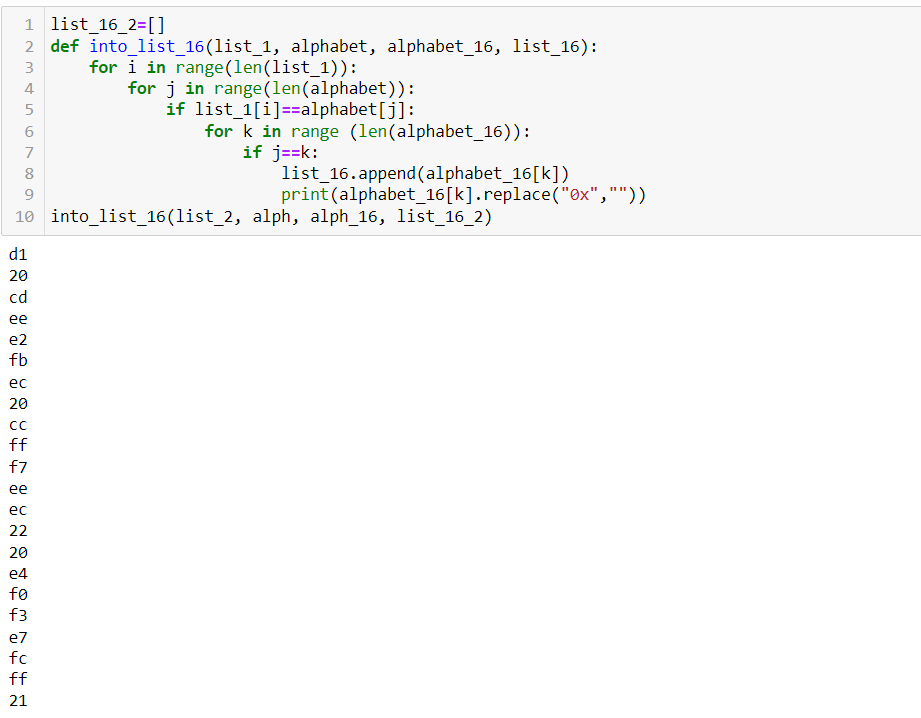


Figure 5: Шестнадцетиричная система

## Шифрование

Зашифровала два сообщения с помощью одного и того же ключа.



Figure 6: Шифрование

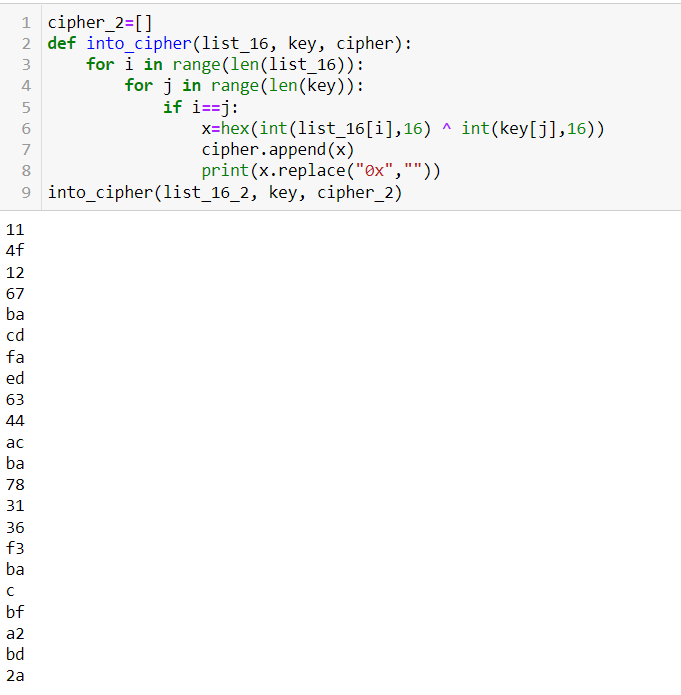


Figure 7: Шифрование

## Способ, прочтения одного из открытых текстов

Способ, при котором злоумышленник может прочитать оба текста, не зная ключа, но зная один из открытых текстов и два зашифровки текстов.

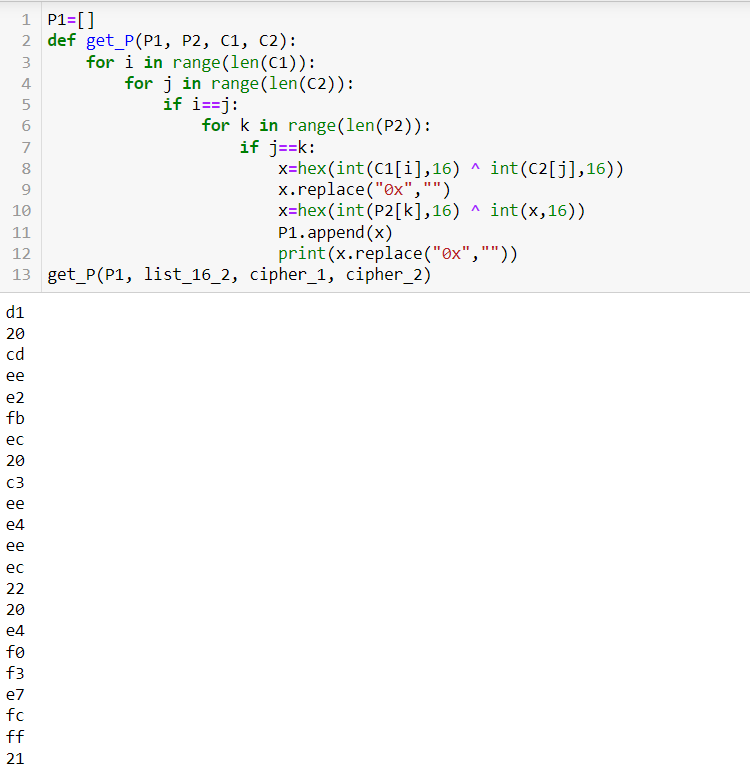


Figure 8: Прочтение

## Проверка

Проверка

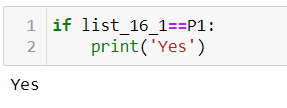


Figure 9: Проверка

# Выводы

Я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.