Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Липатникова М.С. группа НФИбд-02-19

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 Выполнение лабораторной работы

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение (fig. 1), позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно: 1. Определить вид шифротекста при известном ключе и известном откры- том тексте. 2. Определить ключ, с помощью которого шифротекст может быть преоб- разован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Создала 4 функции: - одна генерирует ключ из ASCII-кодов по количеству букв в сообщении; - вторая делает шифрование в режиме однократного гаммирования: сначала каждая буква текста и ключа изменяется на число из таблицы символов Unicode, представляющее его позицию, потом это число переводится в 16-ную систему. Далее текст возводится в степень ключа - это зашифрованное сообщение; - в третьей функции мы можем найти открытый ключ по тексту и зашифрованному тексту; - в четвертой функции находим открытое собщение из зашифрованного и ключа.

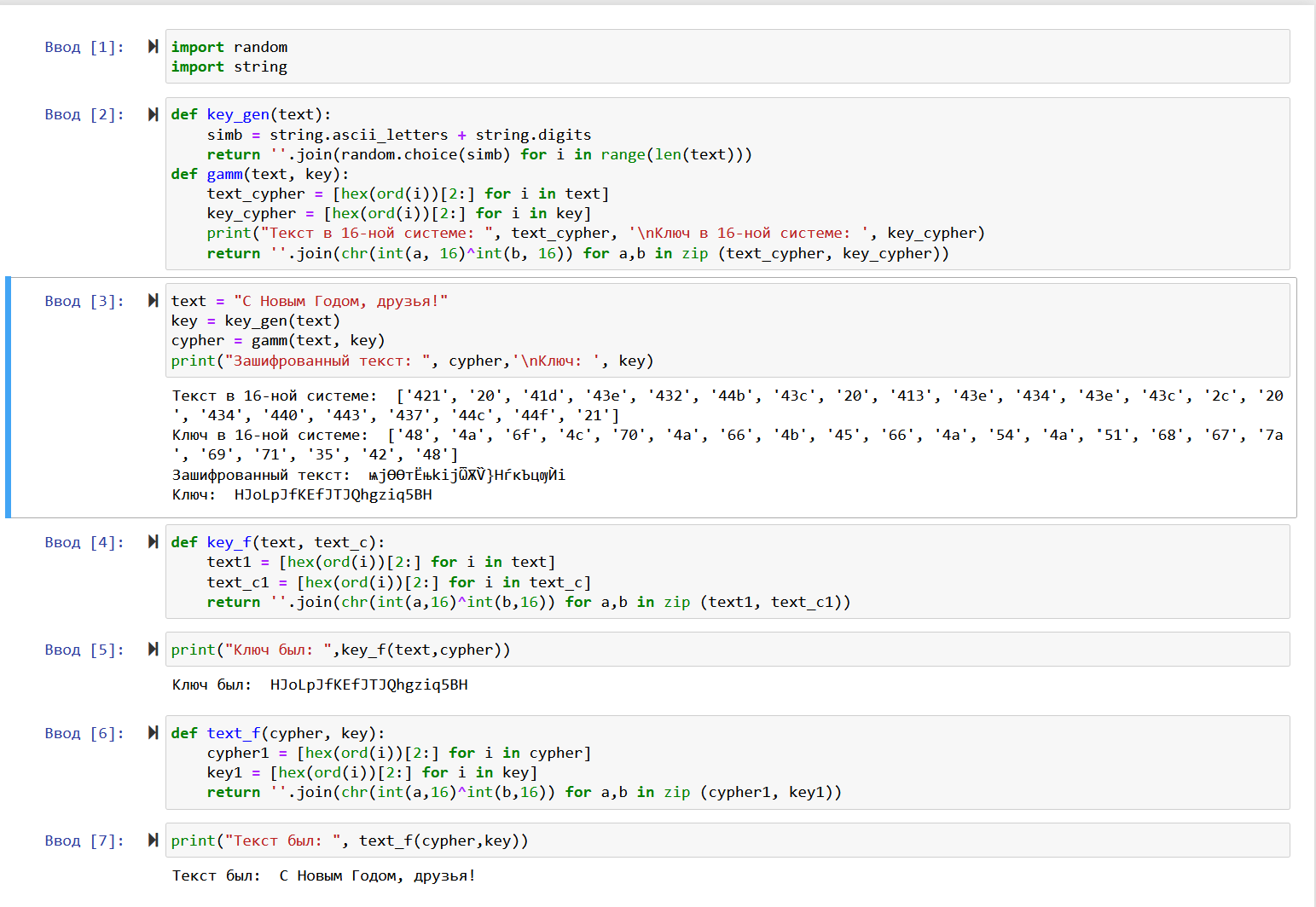


Figure 1: Программа

# 3 Вывод

Освоила на практике применение режима однократного гаммирования.

# 4 Список литературы

1. Теоретические материалы курса.