Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Липатникова М.С. группа НФИбд-02-19

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования (fig. 1). Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить(fig. 2).

Создала 3 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 по двум шифротекстам и тексту-шаблону мы находим позиции, а потом дешифровываем второе сообщение.



Figure 1: Программа

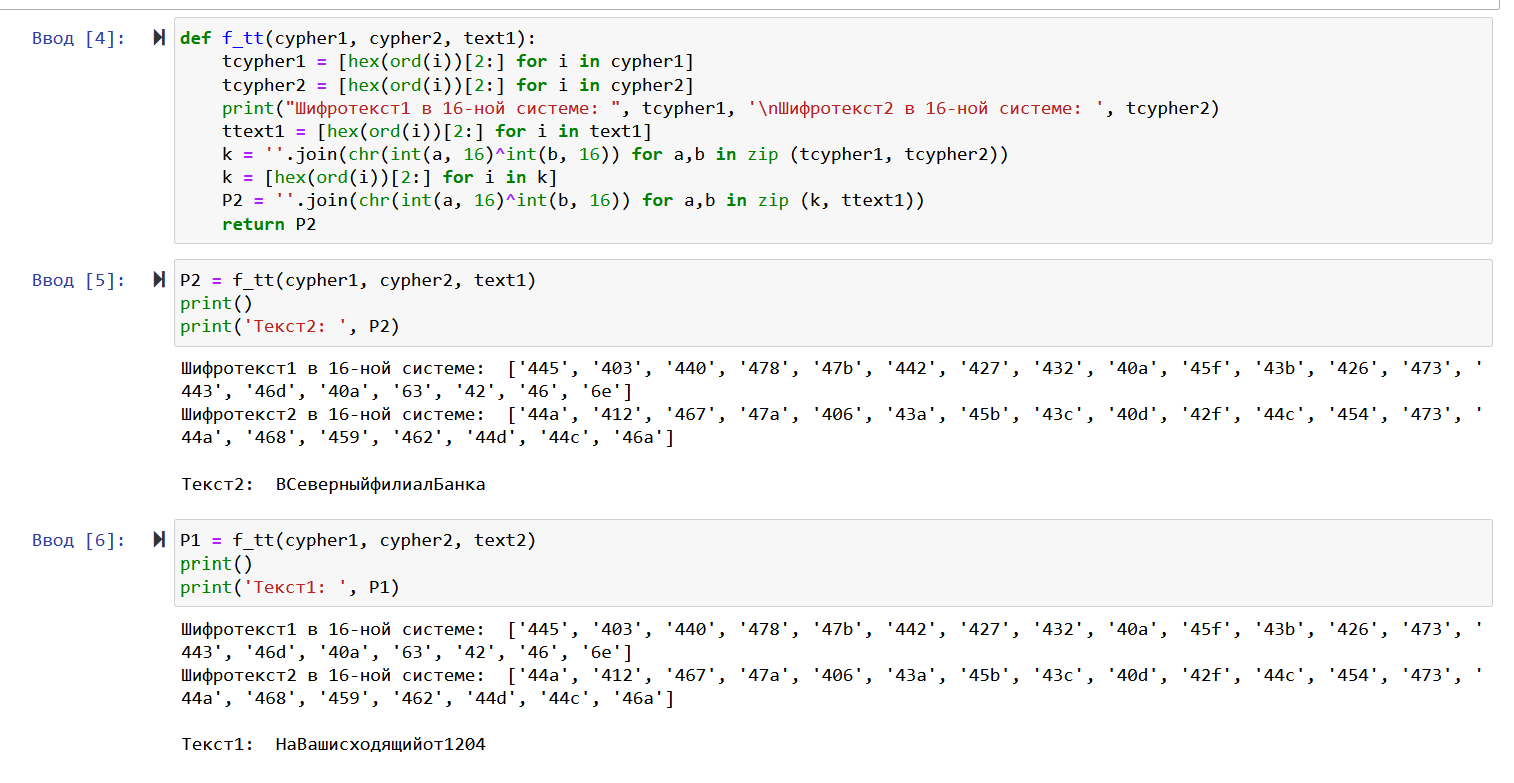


Figure 2: Программа

# 3 Вывод

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

# 4 Список литературы

1. Теоретические материалы курса.