Отчёт по лабораторной работе №8

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

Голощапова Ирина Борисовна

Содержание

# 1 Цель работы

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

# 2 Теоретическое введение

Предложенная Г. С. Вернамом так называемая «схема однократного использования (гаммирования)» является простой, но надёжной схемой шифрования данных. 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.

# 3 Постановка задачи

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. 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.

# 4 Выполнение лабораторной работы

1. Для написания программы использовала язык Python. Для начала импортировала необходимые библиотеки и задала две исходные строки равной длины (рис. [1](#fig:01))

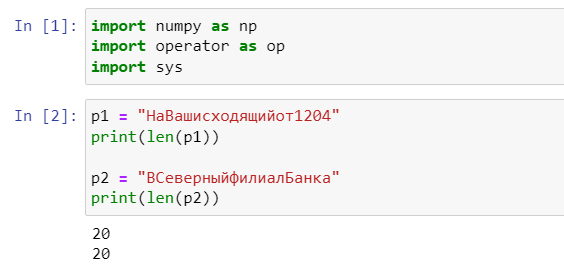


Figure 1: Импорт библиотек и задание исходных данных

1. Написала функцию, которая определяет вид шифротекстов обеих строк при известном ключе(рис. [2](#fig:02))

Функция получает на вход две символьные строки, переводит их в 16-ый форма и генерирует 16-ый ключ. Далее с помощью данного ключа вычисляются шифротексты в 16-ой СС и переводятся в строковый формат.



Figure 2: Функция 1 (шифрование)

1. Проверила работу первой функции (рис. [3](#fig:03))

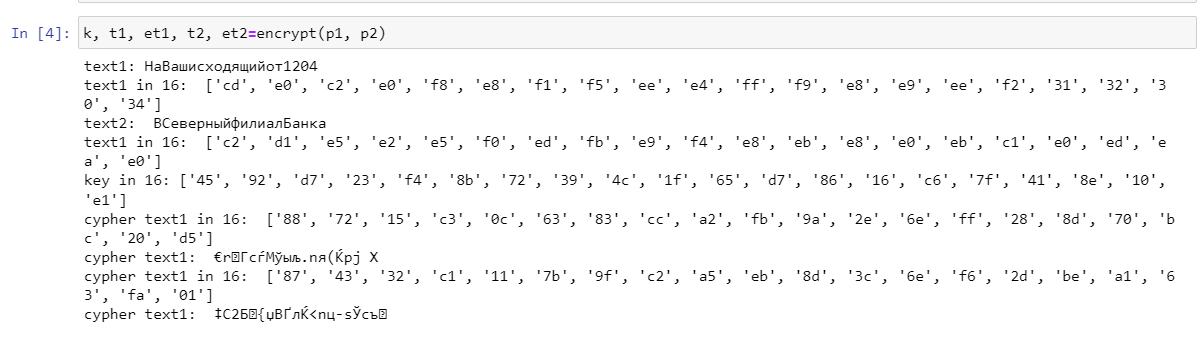


Figure 3: Работа функции шифрования

1. Написала функцию, которая при известных двух шифротекстах и одном открытом тексте находит вид второго открытого текста без ключа (рис. [4](#fig:04))

Функция получает на вход две зашифрованные строки и один открытый текст. Далее шифротексты переводятся в 16-ый формат и применяется принцип однократного гаммирования. Находится вид второго сообщения без использования ключа и возвращается расшифрованное сообщение.



Figure 4: Функция 2 (расшифровка)

1. Проверила работу функции расшифрования (рис. [5](#fig:05))

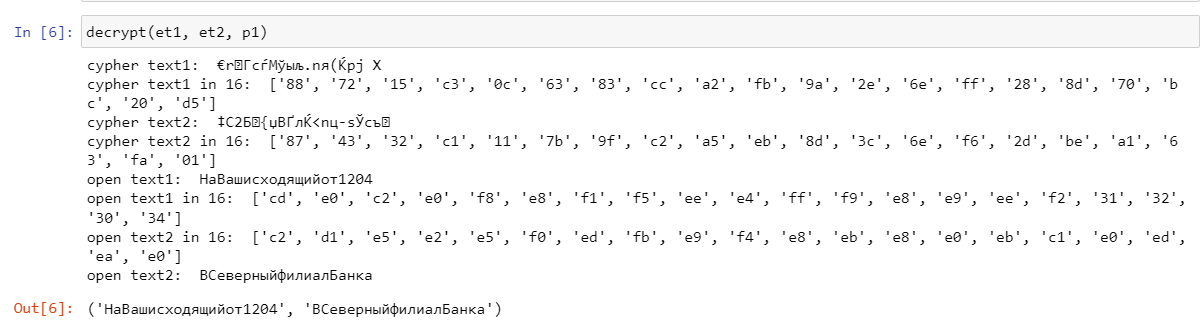


Figure 5: Работа функции расшифрования

# 5 Выводы

В ходе лабораторной работы мне удалось освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# 6 Библиография

1. [Git - система контроля версий](https://github.com/)
2. [Rocky Linux](https://rockylinux.org/)
3. [Элементы криптографии](https://studopedia.su/10_105527_elementi-kriptografii.html)
4. [Однократное гаммирование](https://bugtraq.ru/library/books/crypto/chapter7/)