Отчет по лабораторной работе №8

по дисциплине: Информационная безопасность

Го Чаопэн

Содержание

# Цель работы

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

# Задание

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.

# Теоретическое введение

* Шифрование – это технология кодирования и раскодирования данных.Зашифрованные данные -это результат применения алгоритма для кодирования данных с целью сделать их недоступными для чтения. Данные могут быть раскодированы в исходную форму только путем применения специальный ключа [1].
* Гаммирование — это наложение (или снятие при расшифровке сообщений) на открытое (или зашифрованное) сообщение так называемой криптографической гаммы. Криптографическая гамма — это последовательность элементов данных, которая вырабатывается с помощью определенного алгоритма. [2].

# Выполнение лабораторной работы

1. Создаем функцию шифрования ([1](#fig:001)).

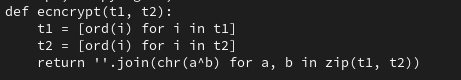


Figure 1: Функция шифрования

1. Введем данные из условия ([2](#fig:002)).

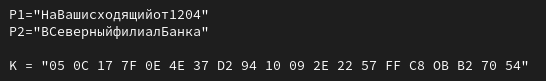


Figure 2: Данные из условия

1. Зашифруем текст с помощью ключа К ([3](#fig:003)).



Figure 3: Шифрование текста

1. Создадим последовательность, с помощью которой будем расшифровывать текст. Передадим ее в функцию шифрования вместе с зашифрованным текстом.

decr = ecncrypt(C1, C2)

1. Запустим программу и получим результат ([4](#fig:004)).

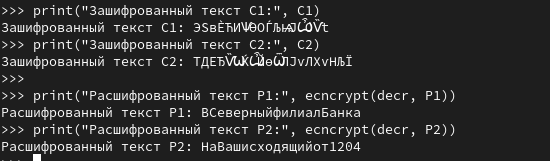


Figure 4: Результат выполнения программы

# Выводы

В рамках данной лабораторной работы было освоено на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Список литературы

1. Шифрование информации: как защитить свои данные [Электронный ресурс]. URL: <https://gb.ru/blog/shifrovanie-informatsii/>.

2. Гаммирование [Электронный ресурс]. URL: <https://science.fandom.com/ru/wiki/%D0%93%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5>.