Отчет по лабораторной работе №8

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

Исаханян Эдуард Тигранович

2022 Sep 21th

Содержание

# Цель работы

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

# Задание

1. Написать программу, которая должна определять вид шифротекстов при известных открытых текстах и при известном ключе;
2. Также эта программа должна определить вид одного из текстов, зная вид другого открытого текста и зашифрованный вид обоих текстов (т.е. не нужно использовать ключ при дешифровке).

# Выполнение лабораторной работы

Напишем функцию шифрования, которая определяет вид шифротекста при известном ключе и известных открытых текстах “ЭкрюельПуаро” и “АртурГастин”. (рис. 1)



Figure 1: Функция, шифрующая данные

А также посмотрим работу данной функции. (рис. 2)

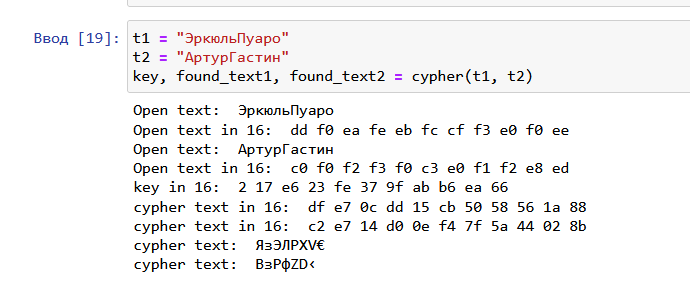


Figure 2: Результат работы функции, шифрующей данные

Напишем функцию дешифровки, которая определяет вид одного из текстов, зная вид другого открытого текста и зашифрованный вид обоих текстов (т.е. не испольузет ключ). (рис. 3)

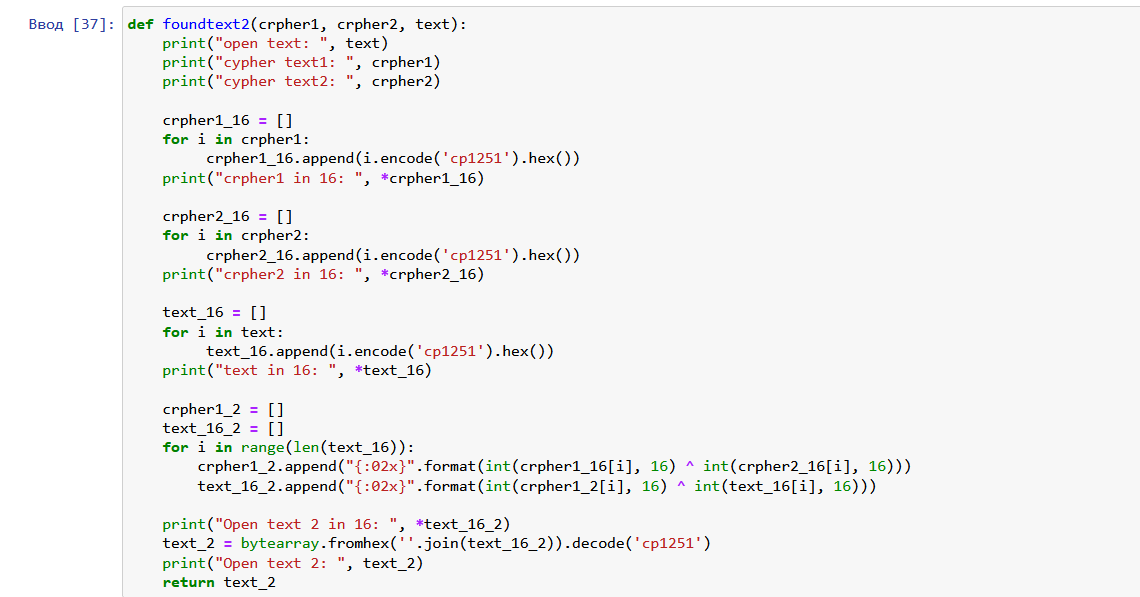


Figure 3: Функция, дешифрующая данные

А также посмторим на результат работы программы при известном тексте “ЭкрюельПуаро”. (рис. 4)

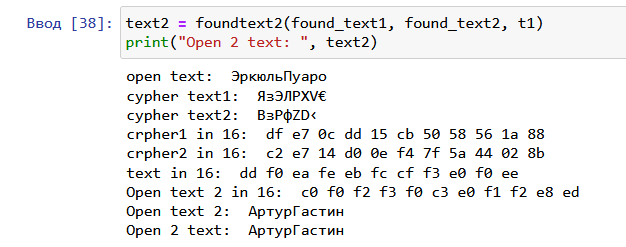


Figure 4: Результат работы функции, дешифрующей данные

И на результат при известном тексте “АртурГастин”. (рис. 5)

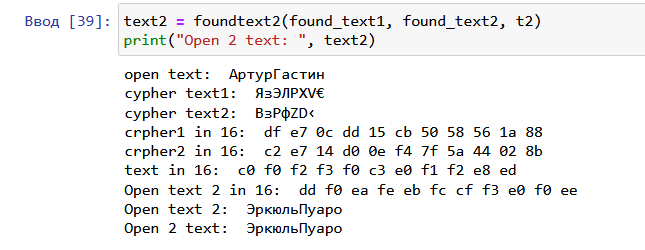


Figure 5: Результат работы функции, дешифрующей данные

## Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?  
   Чтобы определить один из текстов, зная другой, необходимо вопсользоваться следующей формулой: , где и - шифротексты. Т.е. ключ в данной формуле не используется.
2. Что будет при повторном использовании ключа при шифровании текста?  
   При повторном использовании ключа при шифровании текста получим исходное сообщение.
3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?  
   Режим шифрования однократного гаммирования одним ключом двух открытых текстов реализуется по следующей формуле:
4. где - шифротексты, - открытые тексты, - единый ключ шифровки
5. Перечислите недостатки шифрования одним ключом двух открытых текстов.  
   Во-первых, имея на руках одно из сообщений в открытом виде и оба шифротекста, злоумышленник способен расшифровать каждое сообщение, не зная ключа. Во-вторых, зная шаблон сообщений, злоумышленник получает возможность определить те символы сообщения , которые находятся на позициях известного шаблона сообщения .
6. Перечислите преимущества шифрования одним ключом двух открытых текстов.  
   Такой подход помогает упростить процесс шифрования и дешифровки. Также, при отправке сообщений между 2-я компьютерами, удобнее пользоваться одним общим ключом для передаваемых данных

# Выводы

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

# Список литературы

1. Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН” https://esystem.rudn.ru/  
   ::: {#refs} :::