Информационная безопасность.

Лабораторная работа №8.

Филиппова Веорника Сергеевна.

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

Написала функцию шифрования, которая определяет вид шифротекста при известном ключе и известных открытых текстах “НаВашисходящийот1204” и “ВСеверныйфилиалБанка”.



Рисцунок 1

Написала функцию дешифровки, которая определяет вид одного из текстов, зная вид другого открытого текста и зашифрованный вид обоих текстов

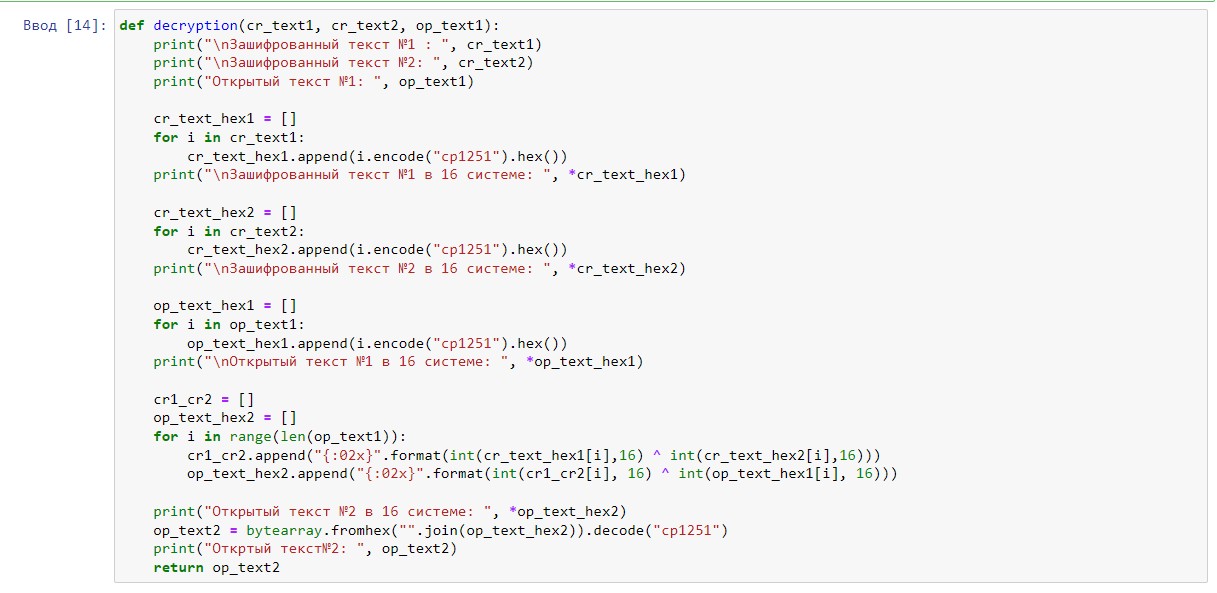


Рисунок 2

Результат функции шифрования.

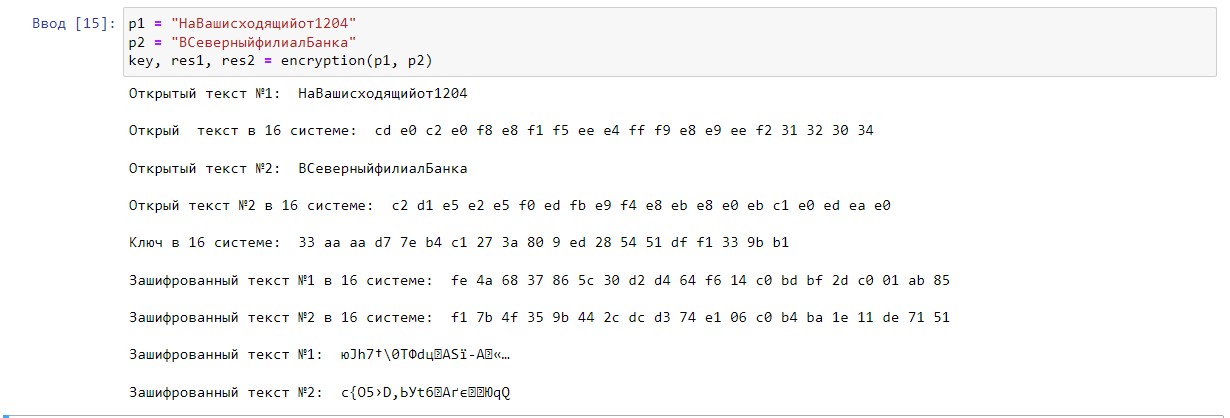


Рисунок 3

Результат функции дешифрования.

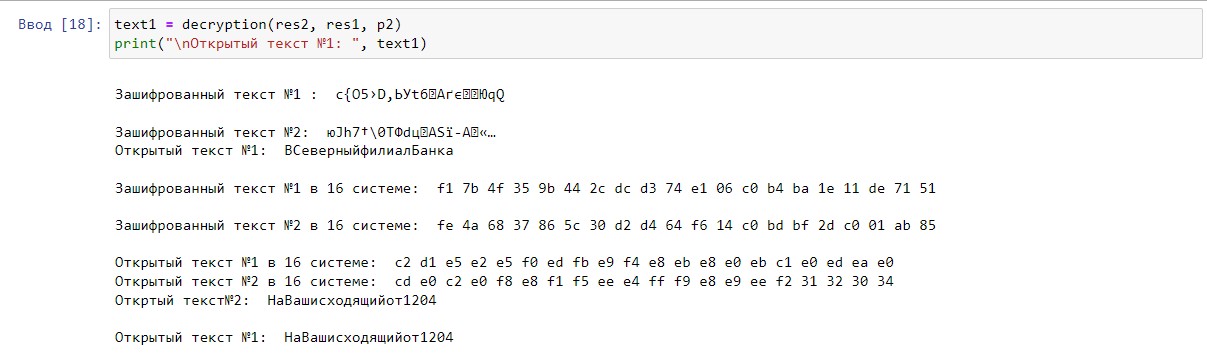


Рисунок 4



Рисунок 5

# Ответы на вопросы

1. Не зная ключа, для определения одного из текстов, зная другой, необходимо воспользоваться формулой: , где и - шифротексты.
2. При повторном использовании ключа при шифровании текста получим исходное сообщение
3. Режим шифрования однократного гаммирования одним ключом двух открытых текстов реализуется по формуле:
4. где - шифротексты, - открытые тексты, - единый ключ шифровки
5. Недостатки шифрования одним ключом двух открытых текстов:
   * Если одно из сообщений доступно в открытом виде и есть оба шифротекста, можно расшифровать каждое сообщение, не зная ключа.
   * Зная шаблон сообщений, есть возможность определить те символы сообщения , которые находятся на позициях известного шаблона сообщения .
6. Преимущества шифрования одним ключом двух открытых текстов:
   * Данный подход помогает упростить процесс шифрования и дешифровки.
   * При отправке сообщений между двумя компьютерами, удобнее пользоваться одним общим ключом для передаваемых данных

# Выводы

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