Лабораторная работа №8

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

Дмитрий Константинович Федотов

Содержание

# Цель работы

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

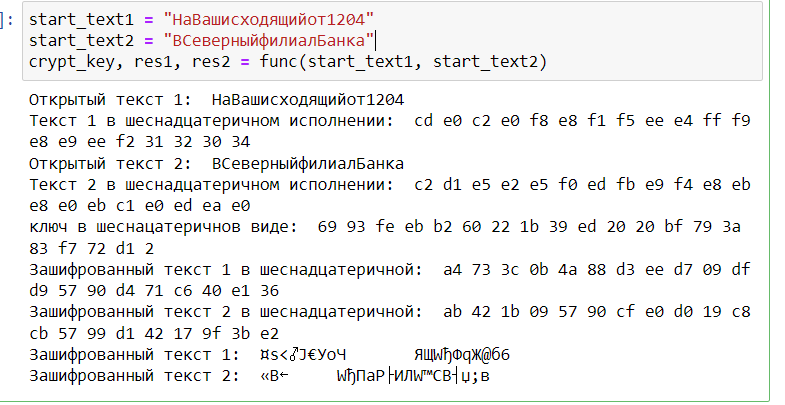
Ответить на вопросы.

# Выполнение лабораторной работы

1. Написал функцию шифрования, которая определяет вид шифротекста при известном ключе и известных открытых текстах (рис - @fig:001), а также работа данной функции (рис - @fig:002).



Функция, шифрующая данные

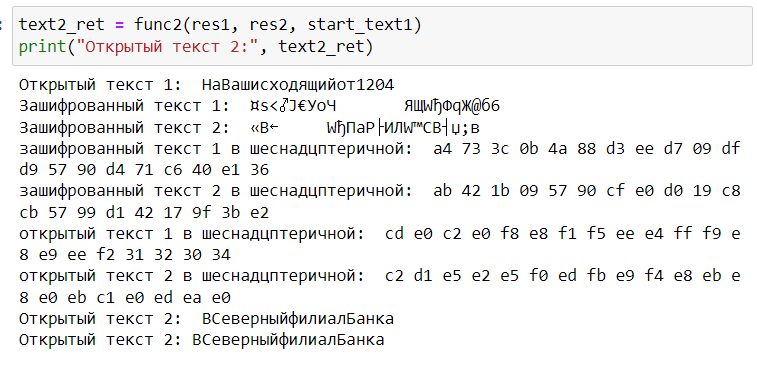


Результат работы функции

1. Написал функцию дешифровки, которая определяет вид одного из текстов, зная вид другого открытого текста и зашифрованный вид обоих текстов, не используя ключ. (рис - @fig:003). А также представил результаты работы программы (рис - @fig:004).



Функция, дешифрующая данные



Результат работы функции

# Выводы

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

# Ответы на контрольные вопросы

1. , где и - шифротексты. Т.е. ключ в данной формуле не используется.
2. При повторном использовании ключа при шифровании текста получим исходное сообщение.
3. с помощью формулы:
4. где - шифротексты, - открытые тексты, - единый ключ шифровки
5. Недостатки шифрования одним ключом двух открытых текстов: Зная одно сообщение и два шифротекста, можно расшифровать без ключа.  
   Зная шаблон сообщений, можно определить те символы сообщения , которые находятся на позициях известного шаблона сообщения .
6. Преимущества шифрования одним ключом двух открытых текстов:  
   Процесс шифровки и дешифровки становится проще. Между двумя компьютерами, удобнее пользоваться одним ключом.