Отчёт по лабораторной работе

**Лабораторная работа №\_08 / Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом**

Габриэль Тьерри

Содержание

# Цель работы………………………………………………………………………………………

# Задание……………………………………………………………………………………………..

# Выполнение лабораторной работы…………………………………………………

# Выводы……………………………………………………………………………………………..

# Цель работы

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

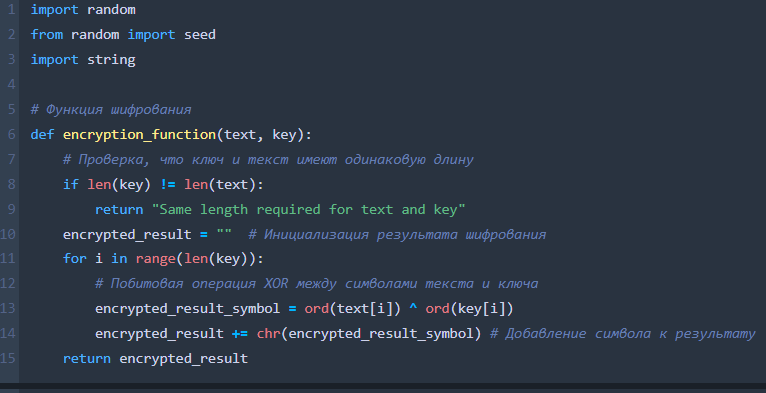
# 

# 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 и в режиме однократного гаммирования. Приложение должно определить вид шифротекстов и обоих текстов и при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

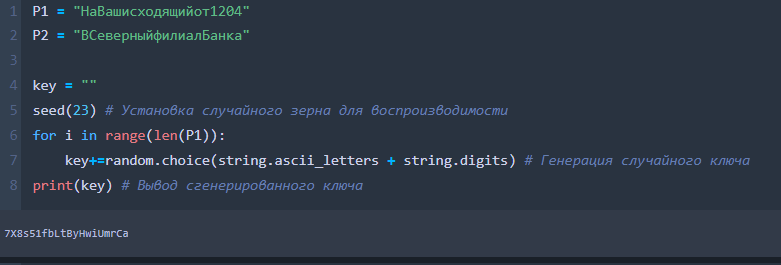
# Выполнение лабораторной работы

Определил функцию шифрования и дешифрования



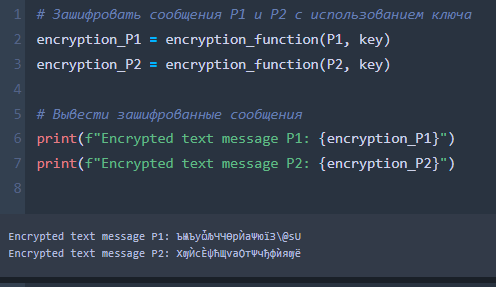
изображение 001

генерируем ключ



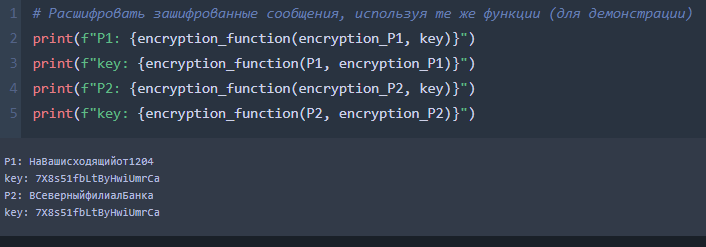
изображение 001

Вызов зашифрованные сообщения



изображение 001

Пример обратного шифрования



изображение 001

# Выводы

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