отчёта по лабораторной работе 7

Элементы криптографии. Однократное гаммирование

Неустроева Ирина Николаевна

Содержание

# 1 Цель работы

Освоить напрактике применение режима однократного гаммирования.

# 2 Выполнение лабораторной работы

В подтверждение выполнения задания прилагаю скриншот кода программы, написанной на языке Python.

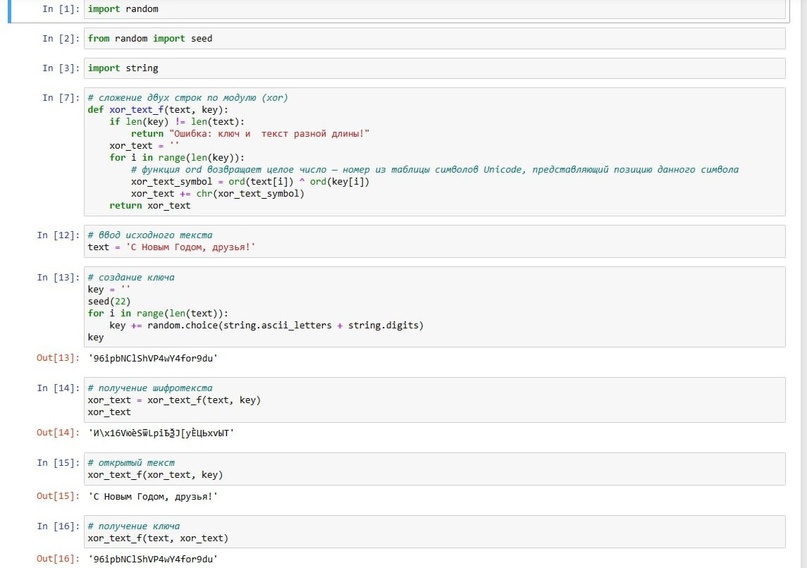


Рис. 1: Программный код

Ключевым элементом этой программы является функция xortextf, которая принимает две строки для сложения. Эти строки должны иметь одинаковую длину, и программа проверяет это условие. Если длины строк различаются, выводится сообщение об ошибке. В случае успешной проверки мы поочередно применяем операцию сложения по модулю к символам строк, в результате чего получаем сумму двух строк.

# 3 Выводы

В процессе выполнения лабораторной работы я овладела навыками шифрования и дешифрования сообщений с использованием однократного гаммирования и познакомилась с этим методом в криптографии.