Отчёт по лабораторной работе №7

Основы информационной безопасности

Надежда Александровна Рогожина

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 Задание

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# 3 Теоретическое введение

*Гаммирование* представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте. Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ⊕) между элементами гаммы и элементами подлежащего сокрытию текста.

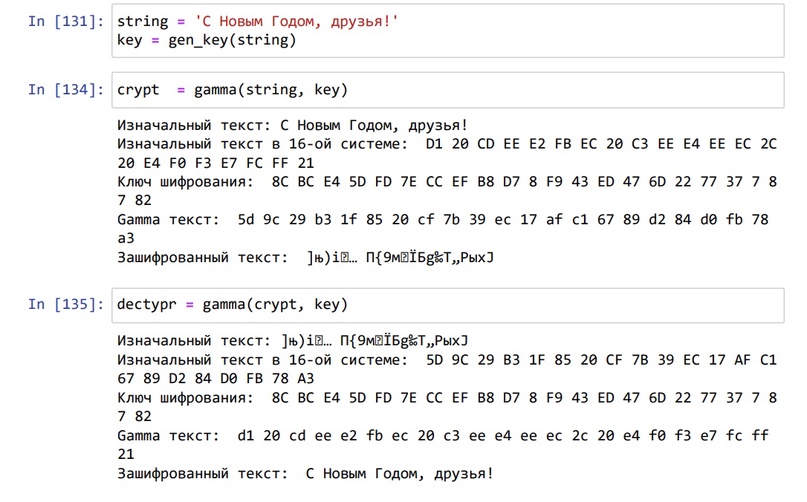
Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой.

# 4 Выполнение лабораторной работы

Код программы:

def gen\_key(string):  
 k = np.random.randint(0, 255, len(string))  
 key = [hex(i)[2:] for i in k]  
 return key  
   
def gamma(string, key):  
 print(f'Изначальный текст: {string}')  
 hex\_str = []  
 for i in string:  
 hex\_str.append(i.encode('cp1251').hex().upper())  
 print(f'Изначальный текст в 16-ой системе: ',\*hex\_str)  
  
 hex\_key = []  
 for i in key:  
 hex\_key.append(i.upper())  
 print(f'Ключ шифрования: ', \*hex\_key)  
   
 gamma = []  
 for i in range(len(hex\_str)):  
 gamma.append('{:02x}'.format(int(hex\_str[i], 16)^int(hex\_key[i], 16)))  
 print(f'Gamma текст: ', \*gamma)  
 cr\_str = bytearray.fromhex(''.join(gamma)).decode('cp1251')  
 print(f'Зашифрованный текст: ', cr\_str)  
 return cr\_str

Пример работы (рис. [??]).



С Новый Годом, друзья!

# 5 Выводы

В ходе лабораторной работы мы написали код для шифрации и дешифрации фразы “С Новым Годом, друзья!”, а также освоили основные принципы однократного гаммирования.

# Список литературы