Отчёт по лабораторной работе №8

дисциплина: Информационная безопасность

Никитаева Александра Семеновна, НПИбд-02-18

Содержание

# Цель работы

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

# Выполнение лабораторной работы

1. Объявила нужные библиотеки. Задала исходные данные – телеграммы Центра.

import numpy as np  
import operator as op  
import sys  
  
P1 = "GimmeGimmeGimmeA"  
P2 = "ManAfterMidnight"

Также вывела длины телеграмм, чтобы показать, что они равны (рис. 1).

print("Длина первой телеграммы {} символов, а второй -- {}".format(len(P1), len(P2)))

Figure 1: Вывод на экран длин телеграмм

Figure 1: Вывод на экран длин телеграмм

1. Написала функцию, кодирующую исходные тексты в режиме однократного гаммирования.

def shifrovka(p1, p2):  
 print("Исходная телеграмма 1: ", p1)  
 print("Исходная телеграмма 2: ", p2)  
   
 p1\_16 = []  
 p2\_16 = []  
 for i in p1:  
 p1\_16.append(i.encode("cp1251").hex())  
 for i in p2:  
 p2\_16.append(i.encode("cp1251").hex())  
 print("Телеграмма 1 в 16-ой форме: ", p1\_16)  
 print("Телеграмма 2 в 16-ой форме: ", p2\_16)  
   
 K = []  
 for i in np.random.randint(0, 255, len(p1)):  
 K.append(hex(i)[2:])  
 print("Ключ длиной {} байт: {}".format(len(p1), K))  
   
 c1\_16 = []  
 c2\_16 = []  
 for i in range(len(p1\_16)):  
 c1\_16.append("{:02x}".format(int(K[i], 16) ^ int(p1\_16[i], 16)))  
 for i in range(len(p2\_16)):  
 c2\_16.append("{:02x}".format(int(K[i], 16) ^ int(p2\_16[i], 16)))  
 print("Зашифрованная телеграмма 1 в 16-ой форме: ", c1\_16)  
 print("Зашифрованная телеграмма 2 в 16-ой форме: ", c2\_16)  
   
 c1 = bytearray.fromhex("".join(c1\_16)).decode("cp1251")  
 c2 = bytearray.fromhex("".join(c2\_16)).decode("cp1251")  
 print("Зашифрованная телеграмма 1: ", c1)  
 print("Зашифрованная телеграмма 2: ", c2)  
 return c1, c2

1. Закодировала исходные тексты (рис. 2).

C1, C2 = shifrovka(P1, P2)

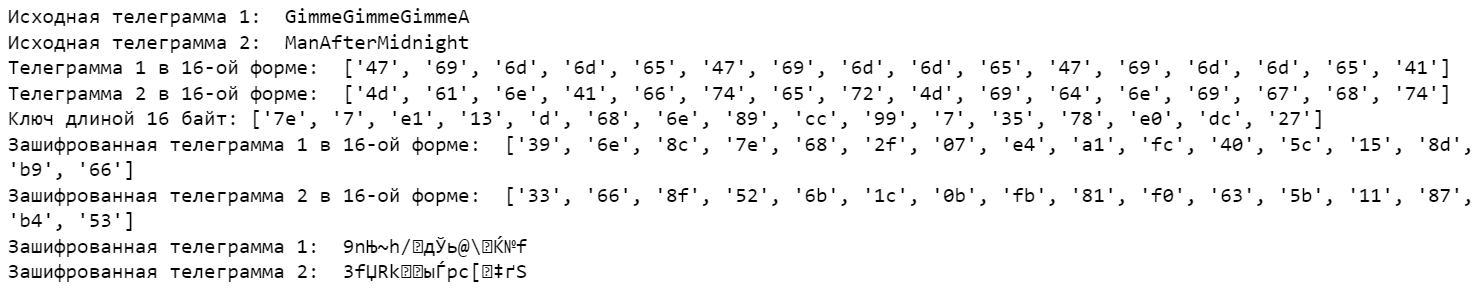


Figure 2: Шифрование исходных телеграмм

1. Написала функцию, читающую (дешифрующую) оба текста, не зная ключа и не стремясь его определить, но получая на вход шаблон.

def rasshifrovka(c1, c2, p):  
 print("Зашифрованная телеграмма 1: ", c1)  
 print("Зашифрованная телеграмма 2: ", c2)  
   
 c1\_16 = []  
 c2\_16 = []  
 for i in c1:  
 c1\_16.append(i.encode("cp1251").hex())  
 for i in c2:  
 c2\_16.append(i.encode("cp1251").hex())  
 print("Зашифрованная телеграмма 1 в 16-ой форме: ", c1\_16)  
 print("Зашифрованная телеграмма 2 в 16-ой форме: ", c2\_16)  
   
 print("Шаблон: ", p)  
   
 p\_16 = []  
 for i in p:  
 p\_16.append(i.encode("cp1251").hex())  
 print("Шаблон в 16-ой форме: ", p\_16)  
   
 tmp = []  
 pp\_16 = []  
 for i in range(len(p)):  
 tmp.append("{:02x}".format(int(c1\_16[i], 16) ^ int(c2\_16[i], 16)))  
 pp\_16.append("{:02x}".format(int(tmp[i], 16) ^ int(p\_16[i], 16)))  
 print("Вторая телеграмма в 16-ой форме: ", pp\_16)  
   
 pp = bytearray.fromhex("".join(pp\_16)).decode("cp1251")  
 print("Вторая телеграмма: ", pp)  
 return pp

1. Прочитала оба текста, используя шаблон 1-ой телеграммы (рис. 3).

P2\_dec = rasshifrovka(C1, C2, P1)

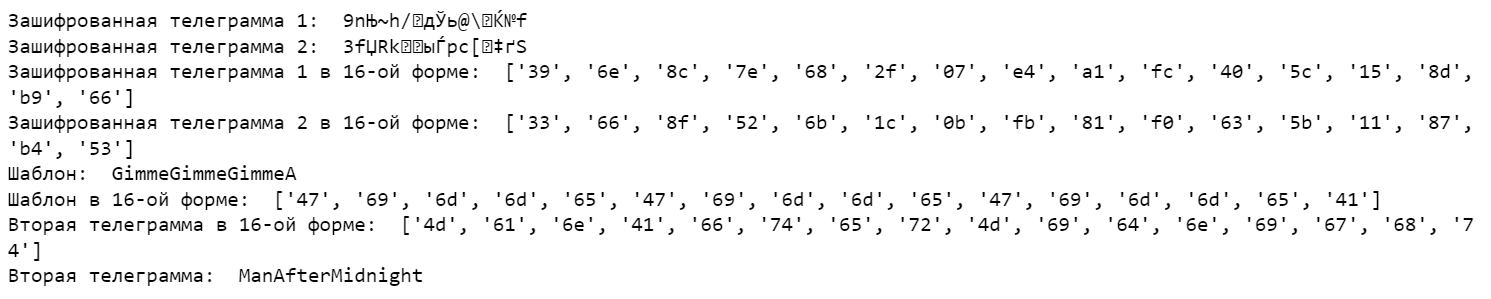


Figure 3: Чтение телеграмм по 1-ой

1. Прочитала оба текста, используя шаблон 2-ой телеграммы (рис. 4).

P1\_dec = rasshifrovka(C1, C2, P2)

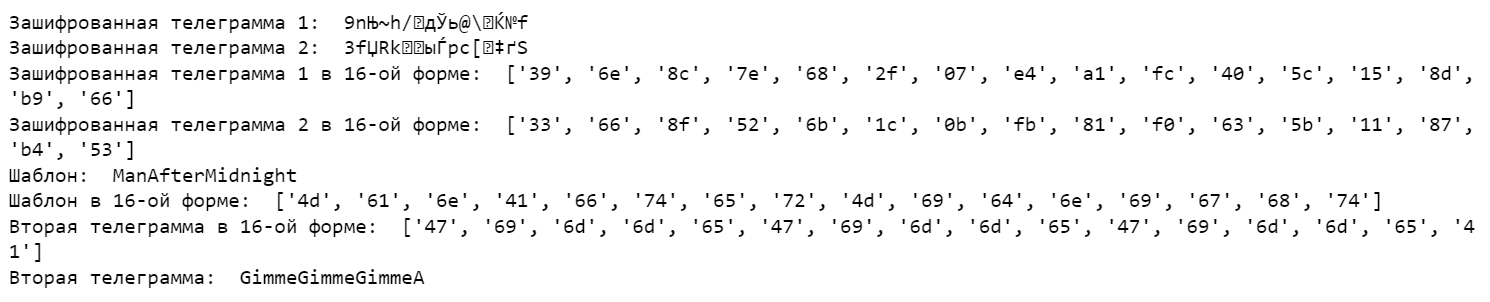


Figure 4: Чтение телеграмм по 2-ой

# Выводы

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

# Ответы на контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?

По формуле (рис. 5):

Figure 5: Определение другого текста

Figure 5: Определение другого текста

1. Что будет при повторном использовании ключа при шифровании текста?

Ничего не изменится – получится исходный текст.

1. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?

По формуле (рис. 6):

Figure 6: Реализация однократного гаммирования

Figure 6: Реализация однократного гаммирования

1. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Злоумышленнику достаточно знать формат хотя бы одного текста и иметь на руках оба шифротекста, чтобы дешифровать послание.

1. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Режим однократного гаммирования помогает упростить процессы шифровки и дешифровки.

# Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом