Отчёт по лабораторной работе №8

дисциплина: Информационная безопасность

Зорин Илья Михайлович

Содержание

# Цель работы

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

# Выполнение лабораторной работы

1. Для выполнения лабораторной работы был использован язык Python.
2. Для реализации алгоритма в начале опишем необходимые функции:

* create\_key: создание ключа
* hexadical\_form: перевод ключа в 16-ичную форму
* gamming: гаммирование

1. Зададим в качестве примера два текста и реализуем алгоритм. Листинг программы выглядит следующим образом: ’’’ #Импортируем необходимые библиотеки import random as rnd import string as str

#Пишем небоходимые функции def create\_key(size=6, chars=str.ascii\_letters + str.digits): return ’’.join(rnd.choice(chars) for \_ in range(size))

def hexadical\_form(s): return ’ ’.join(“{:02x}”.format(ord(c)) for c in s)

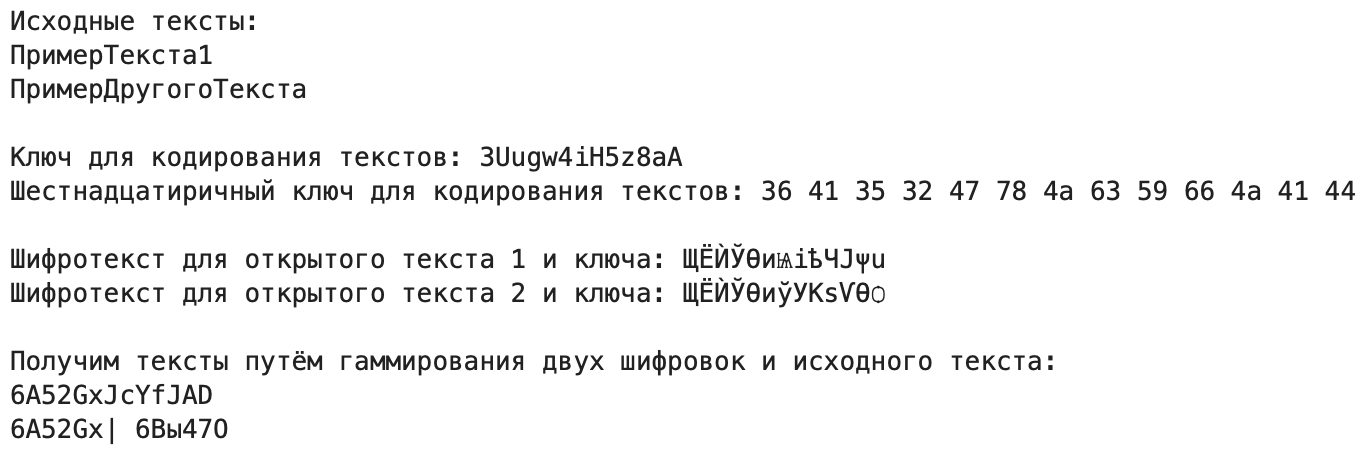
def gamming(fst\_text, sec\_text): fst\_text\_ascii = [ord(i) for i in fst\_text] sec\_text\_ascii = [ord(i) for i in sec\_text] return ’’.join(chr(s^k) for s,k in zip(fst\_text\_ascii,sec\_text\_ascii))

#Выполним шифрование P1, P2 = ‘ПримерТекста1’, ‘ПримерДругогоТекста’ print(‘Исходные тексты:’) print(P1) print(P2)

key=create\_key(len(P1)) print(‘для кодирования текстов:’, create\_key(len(P1))) print(‘Шестнадцатиричный ключ для кодирования текстов:’, hexadical\_form(key))

print(‘для открытого текста 1 и ключа:’, gamming(P1, key)) print(‘Шифротекст для открытого текста 2 и ключа:’, gamming(P2, key))

print(‘тексты путём гаммирования двух шифровок и исходного текста:’) print(gamming(gamming(P1, key)+gamming(P2, key), P1)) print(gamming(gamming(P1, key)+gamming(P2, key), P2)) ’’’

1. Результат выполнения кода: 

# Выводы

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