Лабораторная работа №8

Аминов Зулфикор[1]

29.10, 2022, Москва, Россия

[1]Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

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

Задание к лабораторной работе

Задание

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба тек- ста. Необходимо разработать приложение, позволяющее шифровать и де- шифровать тексты P1 и P2 в режиме однократного гаммирования. Прило- жение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитиче- ски способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Выполнение работы

Программа на python

core.py | pars_somon_tj.py | pars_5ka.py | pars_jeans.py | LR_7.py | test.py | LR_8.py

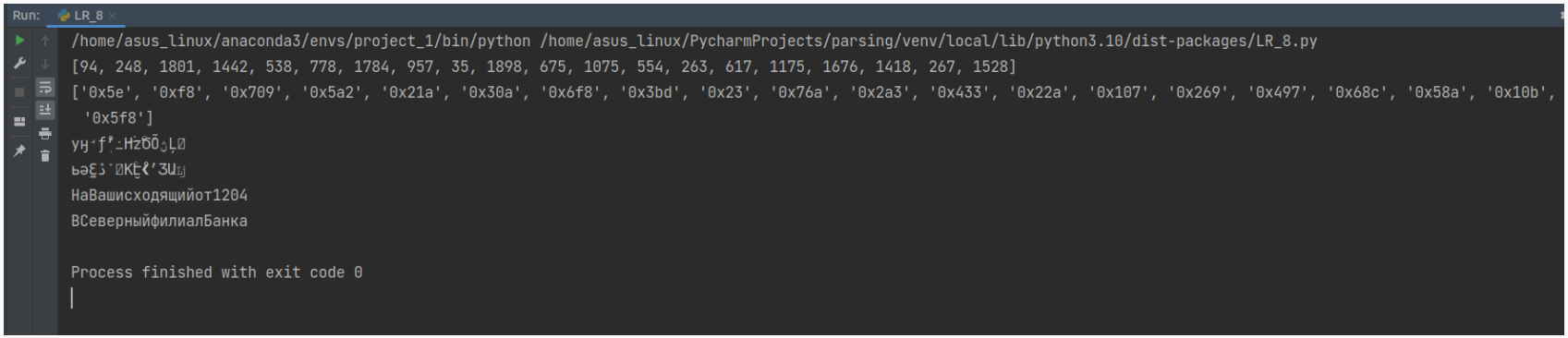
```python
import random
P_1 = "НаВашисходящийот1204"
P_2 = "ВСеверныйфилиалБанка"
def key(text):
    K = []
    for i in range(len(text)):
        K.append(random.randint(0, 2000))
    return K

def hex_key(key):
    h_k = []
    for i in key:
        h_k.append(hex(i))
    return h_k

def encod_and_decod(text, key):
    c = ""
    for i in range(len(text)):
        c += chr(ord(text[i]) ^ key[i])
    return c

k = key(P_1)
print(k)
print(hex_key(k))
c_1 = encod_and_decod(P_1, k)
c_2 = encod_and_decod(P_2, k)
print(c_1)
print(c_2)
print(encod_and_decod(c_1, k))
print(encod_and_decod(c_2, k))
```

Результат работы



Выводы по проделанной работе

Вывод

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