

Лабораторная работа №8

Аминов Зулфикор¹

29.10, 2022, Москва, Россия

¹Российский 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

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

Выполнение работы

Программа на python

```
core.py x pars_somon_tj.py x pars_ska.py x pars_jeans.py x LR_7.py x test.py x LR_8.py x
1  import random
2  P_1 = "НаВашисходящий1204"
3  P_2 = "ВСеверныйфилиалБанка"
4  def key(text):
5      K = []
6      for i in range(len(text)):
7          K.append(random.randint(0, 2000))
8      return K
9
10 def hex_key(key):
11     h_k = []
12     for i in key:
13         h_k.append(hex(i))
14     return h_k
15
16 def encod_and_decod(text, key):
17     c = ""
18     for i in range(len(text)):
19         c += chr(ord(text[i]) ^ key[i])
20     return c
21
22 k = key(P_1)
23 print(k)
24 print(hex_key(k))
25 c_1 = encod_and_decod(P_1, k)
26 c_2 = encod_and_decod(P_2, k)
27 print(c_1)
28 print(c_2)
29 print(encod_and_decod(c_1, k))
30 print(encod_and_decod(c_2, k))
```

Результат работы

```
Run: LR_8
/home/asus_linux/anaconda3/envs/project_1/bin/python /home/asus_linux/PycharmProjects/parsing/venv/local/lib/python3.10/dist-packages/LR_8.py
[94, 248, 1881, 1442, 538, 778, 1784, 957, 35, 1898, 675, 1875, 554, 263, 617, 1175, 1676, 1418, 267, 1528]
['0x5e', '0xf8', '0x709', '0x5a2', '0x21a', '0x30a', '0x6f8', '0x3bd', '0x23', '0x76a', '0x2a3', '0x433', '0x22a', '0x107', '0x269', '0x497', '0x68c', '0x58a', '0x10b',
'0x5f8']
у:ff..H200;|0
ь:63'0Kt'3U|
НаВашисходящий1204
ВСеверныйфилиалБанка

Process finished with exit code 0
```


Выводы по проделанной работе

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