

Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

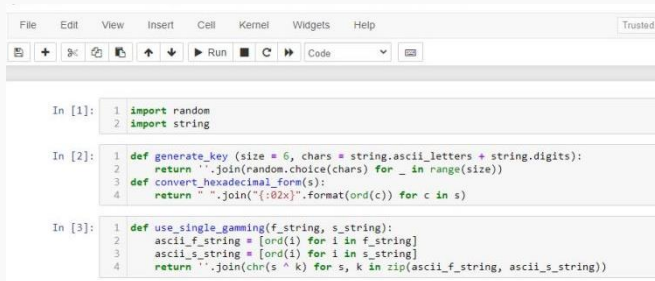
Гудиева Мадина Куйраевна

Цель работы

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

1. Выполнение лабораторной работы
2. Оформление отчета и презентации
3. Выгрузка видео на youtube и файлов на GitHub

Блок программы с библиотеками и функциями



```
File Edit View Insert Cell Kernel Widgets Help Trusted
[Icons] Run Code [Dropdown] [Icon]

In [1]: 1 import random
        2 import string

In [2]: 1 def generate_key (size = 6, chars = string.ascii_letters + string.digits):
        2     return ''.join(random.choice(chars) for _ in range(size))
        3 def convert_hexadecimal_form(s):
        4     return " ".join("{:02x}".format(ord(c)) for c in s)

In [3]: 1 def use_single_gamming(f_string, s_string):
        2     ascii_f_string = [ord(i) for i in f_string]
        3     ascii_s_string = [ord(i) for i in s_string]
        4     return ''.join(chr(s ^ k) for s, k in zip(ascii_f_string, ascii_s_string))
```

Figure 1: Блок программы с библиотеками и функциями

Прочитать оба текста, не зная ключ и не стремясь его определить.

```

Задание
In [4]: 1 P1 = "НаВашисходящийот1204"
2 P2 = "ВСеве́рийфилиалБанка"
3
4 print("P1:", P1)
5 print("P2:", P2)
6
7 K = generate_key(20)
8
9 print("\nK:", K)
10 print("K(16):", convert_hexadecimal_form(K))
11
12 C1 = use_single_gamming(P1, K)
13 C2 = use_single_gamming(P2, K)
14
15 print("\nC1:", C1)
16 print("C1(16):", convert_hexadecimal_form(C1))
17
18 print("\nC2:", C2)
19 print("C2(16):", convert_hexadecimal_form(C2))
20
21 C1C2 = use_single_gamming(C1, C2)
22
23 print("\nВывод текста без ключа:")
24 print("P1:", use_single_gamming(C1C2, P2))
25 print("P2:", use_single_gamming(C1C2, P1))

P1: НаВашисходящийот1204
P2: ВСеве́рийфилиалБанка

K: YwJ2HhInE4ufy5a3glNe6
K(16): 59 77 4a 45 32 68 57 6e 45 34 77 66 79 35 61 33 67 4e 65 36

C1: фчјvQǝXoǝиRcкuV|UǾ
C1(16): 444 447 458 475 47a 450 416 42b 47b 400 438 42f 441 40c 45f 471 56 7c 55 02

C2: ы1ǝVШXǝǝиSc5mT1eиI
C2(16): 44b 456 47f 477 407 428 46a 425 47c 470 44f 45d 441 405 45a 422 457 473 45f 406

Вывод текста без ключа:
P1: НаВашисходящийот1204
P2: ВСеве́рийфилиалБанка

```

Figure 2: Блок программы с выполнением задания

Выводы

Таким образом я успешно освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.