

Лабораторная работа №8

Разважный Георгий НПИбд-02-19

Цель работы

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

Выполнение лабораторной работы

1. Написал код, позволяющий шифровать и дешифровать данные в режиме однократного гаммирования.(рис. 1).

```
1 def create_key(size=6, chars=str.ascii_letters + str.digits):
2     return "".join(rnd.choice(chars) for _ in range(size))
3 def hexadecimal_form(s):
4     return ' '.join("{:02x}".format(ord(c)) for c in s)
5 def gamming(fst_text, sec_text):
6     fst_text_ascii = [ord(i) for i in fst_text]
7     sec_text_ascii = [ord(i) for i in sec_text] return "".join(chr(s^k)
8     for s,k in zip(fst_text_ascii,sec_text_ascii))
9 P1, P2 = "ПримерТекста1", "ПримерДругогоТекста"
10 print('Исходные тексты:')
11 print(P1) print(P2) key=create_key(len(P1))
12 print("длякодирования текстов:", create_key(len(P1)))
13 print("Шестнадцатичный ключ длякодирования текстов:", hexadecimal_form(key))
14 print("для открытого текста 1 и ключа:",gamming(P1, key))
15 print("Шифротекст для открытого текста 2 и ключа:", gamming(P2,key))
16 print("тексты путём гаммирования двух шифровок и исходного текста:")
17 print(gamming(gamming(P1, key)+gamming(P2, key), P1))
18 print(gamming(gamming(P1,key)+gamming(P2, key), P2))
```

Рис.1

Выводы

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