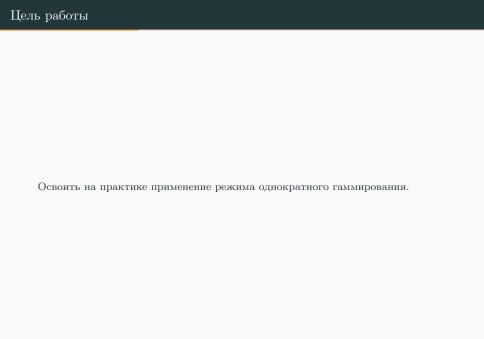
Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Абакумов Егор Александрович



Ход работы

```
In [1]: 1 import random
 2 import string
 4 def generate new key(size = 6, chars = string.ascii letters + string.digits):
       return ''.join(random.choice(chars) for in range(size))
 6 def hexadecimal form(s):
       return " ".join("{:02x}".format(ord(c)) for c in s)
 9 def single_gamming(initial_string, key):
     initial string ascii = [ord(i) for i in initial string]
       key_ascii = [ord(i) for i in key]
       encrypted_string = ''.join(chr(s ^ k) for s, k in zip(initial_string_ascii, key_ascii))
       return encrypted string
14 def unencrypt(encrypted string, key):
       encrypted string ascii = [ord(i) for i in encrypted string]
       key_ascii = [ord(i) for i in key]
    initial string = '.join(chr(s ^ k) for s, k in zip(encrypted string ascii, key ascii))
18 return initial string
19 def compute_initial_key(initial_string, encrypted_string):
20 initial string ascii = [ord(i) for i in initial string]
21
       encrypted_string_ascii = [ord(i) for i in encrypted_string]
       initial_key = '.join(chr(s ^ k) for s, k in zip(initial_string_ascii, encrypted_string_ascii))
       return initial key
```

Блок расчетов переменных

```
In [2]:
  1 initial string = input("Введите начальную строку\n>> ")
  3 kev = generate new key(len(initial string))
  4 print("\nИспользуемый ключ:\n", key)
  5 print("В шестнадцатеричном виде:\n", hexadecimal form(kev))
  7 encrypted string = single gamming(initial string, key)
  9 new key = generate new key(len(encrypted string))
 10 unencrypted new key = unencrypt(encrypted string, new key)
 11 initial key = compute initial key(initial string, encrypted string)
 12 unencrypted initial key = unencrypt(encrypted string, initial key)
Введите начальную строку
>> С Новым Годом, друзья!
Используемый ключ:
 wNyjpNevZlhNAO5mNjwEjP
В шестнадцатеричном виде:
 77 4e 79 6a 70 4e 65 79 5a 6c 68 4e 41 51 35 6d 4e 6a 77 45 6a 50
```

Задание №1

In [3]: 1 print("Полученный при открытом ключе и тексте шифротекст:\n", encrypted_string) print("В шестнадцатеричном виде:\n", hexadecimal_form(encrypted_string))

Полученный при открытом ключе и тексте шифротекст:

inКєтЅљҮщђќΨѽ}ШљЎЩрЉХq В шестнадцатеричном виде:

456 6e 464 454 442 405 459 59 449 452 45c 470 47d 7d 15 459 40e 429 440 409 425 71



В ходе работы мы успешно на практике освоили применение режима однократного гаммирования.