

# Лабораторная работа № 7

Элементы криптографии. Однократное  
гаммирование

Миленин Иван Витальевич

# Цель работы

Освоить на практике применение режима однократного гаммирования.

## **ХОД РАБОТЫ**

# Блок функций для расчетов

```
In [1]: 1 import random
2 import string
3
4 def generate_new_key(size = 6, chars = string.ascii_letters + string.digits):
5     return ''.join(random.choice(chars) for _ in range(size))
6 def hexadecimal_form(s):
7     return " ".join("{:02x}".format(ord(c)) for c in s)
8
9 def single_gamming(initial_string, key):
10     initial_string_ascii = [ord(i) for i in initial_string]
11     key_ascii = [ord(i) for i in key]
12     encrypted_string = ''.join(chr(s ^ k) for s, k in zip(initial_string_ascii, key_ascii))
13     return encrypted_string
14 def unencrypt(encrypted_string, key):
15     encrypted_string_ascii = [ord(i) for i in encrypted_string]
16     key_ascii = [ord(i) for i in key]
17     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]
22     initial_key = ''.join(chr(s ^ k) for s, k in zip(initial_string_ascii, encrypted_string_ascii))
23     return initial_key
```

# Блок расчетов переменных

```
In [2]: 1 initial_string = input("Введите начальную строку\n>> ")
        2
        3 key = generate_new_key(len(initial_string))
        4 print("\nИспользуемый ключ:\n", key)
        5 print("В шестнадцатеричном виде:\n", hexadecimal_form(key))
        6
        7 encrypted_string = single_gamming(initial_string, key)
        8
        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:  
wNyjpNeyZlhNAQ5mNjwEjP  
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

## Задание №1

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

Полученный при открытом ключе и тексте шифротекст:

inKєтSьYщŋĸΨŃ}ѠьŸщрЬXq

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

# Задание №2

## Задание №2

```
In [4]: 1 print("Ключ, преобразовывающий шифротекст в один из возможных вариантов:\n", new_key)
2 print("Один из вариантов прочтения открытого текста:\n", unencrypted_new_key)
3
4 print("\nИсходный ключ:\n", initial_key)
5 print("Расшифрованный исходным ключом шифротекст:\n ", unencrypted_initial_key)
```

Ключ, преобразовывающий шифротекст в один из возможных вариантов:

nKLteDoQmVnKcEUDZJvc1D

Один из вариантов прочтения открытого текста:

и%ШРЧсФФвл08@HeЪЖЖщ5

Исходный ключ:

wNyjpNeyZlhNAQ5mNjwEjP

Расшифрованный исходным ключом шифротекст:

С Новым Годом, друзья!

# Вывод

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