# Лабораторная работа № 7

## Элементы криптографии. Однократное гаммирование

Абакумов Егор Александрович

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Ход работы

# Блок функций для расчетов

In [1]:

```python
import random
import string

def generate_new_key(size = 6, chars = string.ascii_letters + string.digits):
    return ''.join(random.choice(chars) for _ in range(size))
def hexadecimal_form(s):
    return " ".join("{:02x}".format(ord(c)) for c in s)

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
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))
    return initial_string
def compute_initial_key(initial_string, encrypted_string):
    initial_string_ascii = [ord(i) for i in initial_string]
    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]:

```
initial_string = input("Введите начальную строку\n>> ")

key = generate_new_key(len(initial_string))
print("\nИспользуемый ключ:\n", key)
print("В шестнадцатеричном виде:\n", hexadecimal_form(key))

encrypted_string = single_gamming(initial_string, key)

new_key = generate_new_key(len(encrypted_string))
unencrypted_new_key = unencrypt(encrypted_string, new_key)
initial_key = compute_initial_key(initial_string, encrypted_string)
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:
 inЌєтSљYщЋќΨ̊}ЋљЎщрљXq
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]:

```
print("Ключ, преобразовывающий шифротекст в один из возможных вариантов:\n", new_key)
print("Один из вариантов прочтения открытого текста:\n", unencrypted_new_key)

print("\nИсходный ключ:\n", initial_key)
print("Расшифрованный исходным ключом шифротекст:\n ", unencrypted_initial_key)
```

```
Ключ, преобразовывающий шифротекст в один из возможных вариантов:
 nKLteDoQmvnKcEUDZJVclD
Один из вариантов прочтения открытого текста:
 и%ШРЧсФФвлО8@НєЂЖЖщ5

Исходный ключ:
 wNyjpNeyZlhNAQ5mNjwEjP
Расшифрованный исходным ключом шифротекст:
  С Новым Годом, друзья!
```

# Вывод

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