

Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Абдуллаев Сайидазизхон Шухратович

Освоить на практике применение режима однократного гаммирования

Ход работы

Импорт библиотек и написание функций

```
In [1]: import random
import string

In [2]: def gen_key(length, symbols = string.ascii_letters + string.digits):
    return ''.join(random.choice(symbols) for i in range(length))
def gamming(text, key):
    text_conv = [ord(i) for i in text]
    key_conv = [ord(i) for i in key]
    return ''.join(chr(a^b) for a, b in zip(text_conv, key_conv))
```

```
In [4]: text = "С Новым Годом, друзья!"  
key = gen_key(len(text))  
text_shifr = gamming(text, key)  
print ("Шифротекст имеет вид:", text_shifr)
```

Шифротекст имеет вид: ёа1ъьвфџкдсУjI'МлпN

```
In [5]: ganning(ganning(text, key), key)
```

```
Out[5]: 'С Новы Годом, друзья!'
```

```
In [6]: key_2 = gen_key (len(text))  
text_2 = gamming(text_shifr, key_2)  
print ("Расшифрованный текст:" , text_2)
```

Расшифрованный текст: Й+ЗЙГЪ#ФДЦМЛ @a!xГVq@

- В результате выполнения данной работы было освоено на практике применение режима однократного гаммирования