

Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Аксёнова Алина Владимировна

Освоить на практике применение режима однократного гаммирования

Ход работы

```
In [2]: 1 import random
        2 import string

In [11]: 1 def generate_key(length, symbols = string.ascii_letters + string.digits):
        2     return ''.join(random.choice(symbols) for i in range(length))
        3 def gamming(text, key):
        4     text_conv = [ord(i) for i in text]
        5     key_conv = [ord(i) for i in key]
        6     return ''.join(chr(a ^ b) for a, b in zip(text_conv, key_conv))
```

```
In [14]: 1 text = 'С Новым Годом, друзья!'
          2 key = generate_key (len(text))
          3 text_shifr = gamming(text, key)
          4 print ('вид шифротекста:', text_shifr) .
```

вид шифротекста: ГЮЮψгs@iғψЮx1ЪЪSэиЪd

```
In [15]: 1 gamming(gamming(text, key), key)
```

```
Out[15]: 'С Новым Годом, друзья!'
```

```
In [16]: 1 key_2 = generate_key (len(text))
          2 text_2 = gamming(text_shifr, key_2)
          3 print ('Расшифрованный текст:', text_2)
```

Расшифрованный текст: ы'žeOIБ&ЮЇыфпАѢћяыйъj>

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