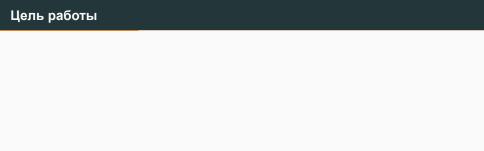
Лабораторная работа № 7

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, simbols = string.ascii letters * string.digits):
    return ''.join(random.choice(simbols) for i in range(length))
    def gaming(text, key):
        text_conv = lord(j for i in text]
        key_conv = [ord(j) for i in key]
        return ''.join(chr(a^h) for a, b in zip(text_conv, key_conv))
```

Шифрование открытого текста

```
In [4]: text = "C Homa Годом, дружья!"

key = pen_key(len(text))

text_shifr = gamming(text, key)

print ("шифрогекст имеет вид:", text_shifr)

шифрогекст имеет вид: "èalushuh@imig(VjTMunmy)

шифрогекст имеет вид: èalushuh@imig(VjTMunmy)

»
```

Проверка правильности работы кода

```
In [5]: gamming(gamming(text, key), key)
Out[5]: "С новы годом, друзья!"
```

Расшифровка зашифрованного текста новым ключом

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

Вывод

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