Защита лабораторной работы №7. Элементы криптографии. Однократное гаммирование

Бармина Ольга Константиновна

2022 Sep 22th

RUDN University, Moscow, Russian Federation

Результат выполнения лабораторной работы №7

Цель выполнения лабораторной работы

Освоить на практике применение режима однократного гаммирования.

Результат выполнения лабораторной работы

```python
def f1(text):
    return ' '.join(hex(ord(i))[2:] for i in text)
```

```python
def f2(size):
    return ' '.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))
```

```python
def f3(text, key):
    return ' '.join(chr(a^b) for a,b in zip(text, key))
```

```python
def f4(text, enc):
    return ' '.join(chr(a^b) for a,b in zip(text, enc))
```

Figure 1: рис 1. функции

Результат выполнения лабораторной работы

```
msg = "С Новым Годом, друзья!"
key = f2(len(msg))
hex_key = f1(key)
print(key)
print(hex_key)
```

```
j L O P b S q m u L X c c 1 h M E C W r M b
6a 20 4c 20 4f 20 50 20 62 20 53 20 71 20 6d 20 75 20 4c 20 58 20 63 20 63 20 31 20 68 20 4d 20 45 20 43 20 57 20 72 20 4d 20 6
2
```

Figure 2: рис 2. задание ключа

Результат выполнения лабораторной работы

```
enc = f3([ord(i) for i in msg], [ord(i) for i in key])
hex_enc = f1(enc)
hex_enc
```

```
'44b 20 0 20 451 20 41e 20 47d 20 46b 20 46c 20 0 20 471 20 41e 20 467 20 41e 20 44d 20 c 20 4d 20 414 20 435 20 463 20 47b 20
46c 20 417 20 1'
```

```
decr = f3([ord(i) for i in enc], [ord(i) for i in key])
print(decr)
```

```
С Новым Годом, друзья!
```

Figure 3: рис 3. зашифрованный текст

Результат выполнения лабораторной работы

```
key2 = f4([ord(i) for i in msg], [ord(i) for i in enc])
decr2 = f3([ord(i) for i in enc], [ord(i) for i in key2])
print(decr2)
```

```
С Новым Годом, друзья!
```

Figure 4: рис 4. расшифрованный текст

Вывод

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