Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование

Волков Тимофей Евгеньевич НПИбд-01-18

Цель работы

Освоить на практике применение режима однократного гаммирования.

Функции

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

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

Ввод [3]:
```
def gen_key(size):
    return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(size))
```

Ввод [4]:
```
def encrypt(text, key):
    return ''.join(chr(a^b) for a, b in zip(text, key))
```

Ввод [5]:
```
def decrypt(encrypt, key):
    return ''.join(chr(a^b) for a, b in zip(encrypt, key))
```

Ввод [6]:
```
def compute_key(text, encrypt):
    return ''.join(chr(a^b) for a, b in zip(text, encrypt))
```

Figure 1: Функции

Задание 1

Ввод [7]:

```
text = 'С Новым Годом, друзья!'

key = gen_key(len(text))
hex_key = hex_(key)

print("Ключ: ", hex_key)

encrypt = encrypt([ord(i) for i in text], [ord(i) for i in key])
hex_encrypt = hex_(encrypt)

print("Зашифрованное сообщение: ", hex_encrypt)

decrypt_ = decrypt([ord(i) for i in encrypt], [ord(i) for i in key])

print("Расшифрованное сообщение: ", decrypt_)
```

```
Ключ:  63 50 6c 65 33 34 71 69 49 54 58 55 67 41 51 6d 59 6b 78 74 74 72
Зашифрованное сообщение:  442 70 471 45b 401 47f 44d 49 45a 46a 46c 46b 45b 6d 71 459 419 428 44f 438 43b 53
Расшифрованное сообщение:  С Новым Годом, друзья!
```

Figure 2: Задание 1

Задание 2

Ввод [8]:
```
compute_key = compute_key([ord(i) for i in text], [ord(i) for i in encrypt])

decrypt_compute_key = decrypt([ord(i) for i in encrypt], [ord(i) for i in compute_key])

print("Вариант прочтения открытого текста: ", decrypt_compute_key)
```

```
Вариант прочтения открытого текста:  С Новым Годом, друзья!
```

Figure 3: Задание 2