Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование

Ильин Никита Евгеньевич, НФИбд-01-19

Содержание

List of Figures

List of Tables

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Задание

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

3 Выполнение работы

1. Была написана программа, которая соответствует требоваиям задачи, и проверяет полученный ключ с изначально сгенерированным.

```
import numpy as np
```
✓ 0.5s

```
def encrypt(text):
    print("Открытый текст: ", text)

    text_arr = []
    for i in text:
        text_arr.append(i.encode("cp1251").hex())

    print("Текст в шестнадцатиричном представлении: ", *text_arr)

    key_dec = np.random.randint(0, 255, len(text))
    key_hex = [hex(i)[2:] for i in key_dec]
    print("Ключ в шестнадцатиричном представлении: ", *key_hex)

    text_crypt = []
    for i in range(len(text_arr)):
        text_crypt.append("{:02x}".format(int(text_arr[i], 16) ^ int(key_hex[i], 16)))
    print("Зашифрованный текст в шестнадцатиричном представлении: ", *text_crypt)

    text_fin = bytearray.fromhex("".join(text_crypt)).decode("cp1251")
    print("Зашифрованный текст: ", text_fin)

    return key_hex, text_fin
```
✓ 0.3s

Figure 3.1: функция шифрования

```python
def decrypt(text, text_fin):
    print("Открытый текст: ", text)
    print("Зашифрованный текст: ", text_fin)

    hex_text = []
    for i in text:
        hex_text.append(i.encode("cp1251").hex())
    print("Открытый текст в шестнадцатиричном представлении: ", *hex_text)

    hex_text_fin = []
    for i in text_fin:
        hex_text_fin.append(i.encode("cp1251").hex())
    print("Зашифрованный текст в шестнадцатиричном представлении: ", *hex_text_fin)

    key = [hex(int(i, 16) ^ int(j, 16))[2:] for (i, j) in zip(hex_text, hex_text_fin)]
    print("Полученный ключ в шестнадцатиричном представлении: ", *key)

    return key
```

✓ 0.3s

Figure 3.2: функция расшифровки

```python
text = "С Новым Годом, друзья!"
key_encr, text_crypt = encrypt(text)
```

[71] ✓ 0.3s

```
Открытый текст:  С Новым Годом, друзья!
Текст в шестнадцатиричном представлении:  d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21
Ключ в шестнадцатиричном представлении:  bf f1 b5 2f d8 a7 a5 69 2c d5 12 7a 79 42 79 44 45 99 5e 3e d8 3a
Зашифрованный текст в шестнадцатиричном представлении:  6e d1 78 c1 3a 5c 49 49 ef 3b f6 94 95 6e 59 a0 b5 6a b9 c2 27 1b
Зашифрованный текст:  nСхБ:\IIn;ц”•nY µj‰B'
```

```python
key = decrypt(text, text_crypt)
```

[72] ✓ 0.1s

```
Открытый текст:  С Новым Годом, друзья!
Зашифрованный текст:  nСхБ:\IIn;ц”•nY µj‰B'
Открытый текст в шестнадцатиричном представлении:  d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21
Зашифрованный текст в шестнадцатиричном представлении:  6e d1 78 c1 3a 5c 49 49 ef 3b f6 94 95 6e 59 a0 b5 6a b9 c2 27 1b
Полученный ключ в шестнадцатиричном представлении:  bf f1 b5 2f d8 a7 a5 69 2c d5 12 7a 79 42 79 44 45 99 5e 3e d8 3a
```

```python
print("Ключ верный") if key_encr == key else print("Ключ не подошел")
```

[73] ✓ 0.9s

```
Ключ верный
```

Figure 3.3: Работа программы

4 Выводы

Освоено на практике применение режима однократного гаммирования.

5 Библиография

1. Методические материалы курса