Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Александр Олегович Воробьев

Содержание

1 Цель работы

Освоить на практике применение режима однократного гаммирования

2 Последовательность выполнения работы

1. Блок функции для расчетов.

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

In [5]: def f1(text):
            return " ".join(hex(ord(i))[2:] for i in text)

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

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

        def f4(text, encrypt):
            return "".join(chr(a^b) for a, b in zip (text, encrypt))
```

Figure 2.1: Блок функции для расчетов

2. Определил вид шифротекста при известном ключе и известном открытом тексте.

```
In [6]: message = "С Новым Годом, друзья!"

        key = f2(len(message))
        hex_key = f1(key)

        print("ключ:", key)
        print("шеснадцатеричный ключ:", hex_key)

        encrypt = f3([ord(i) for i in message], [ord(i) for i in key])
        hex_encrypt = f1(encrypt)

        print("зашифрованной сообщение:", hex_encrypt)

        decrypt = f3([ord(i) for i in encrypt], [ord(i) for i in key])

        print("расшифрованное сообщение", decrypt)

ключ: ZW6dbCfxYo371XFXgwmTq5
шеснадцатеричный ключ: 5a 57 36 64 62 43 66 78 59 6f 33 37 31 58 46 58
67 77 6d 54 71 35
зашифрованной сообщение: 47b 77 42b 45a 450 408 45a 58 44a 451 407 409
40d 74 66 46c 427 434 45a 418 43e 14
расшифрованное сообщение С Новым Годом, друзья!
```

Figure 2.2: Получение шифротекста

3. Определил ключ,с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста,представляющий собой один из возможных вариантов прочтения открытого текста.

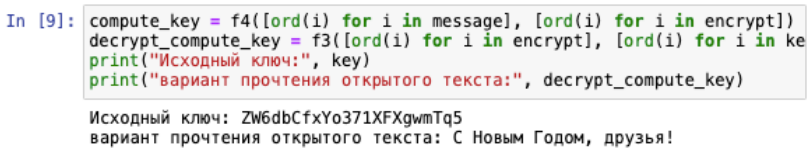

Figure 2.3: Прочтение открытого текста

3 Выводы

Освоил на практике применение режима однократного гаммирования.