Отчёт

по лабораторной работе 7

Лекомцева Алёна

Содержание

Цель работы

Освоить на практике применение режима однократного гаммирования.

Задание

Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

Выполнение лабораторной работы

1. Разработаем приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. (рис.1).

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

In [2]: def generate_key (length, simbols = string.ascii_letters + string.digits):
            return ''.join(random.choice(simbols) for i in range (length))
        def gamming (text, key):
            text_shifr = [ord(i) for i in text]
            key_shifr = [ord(i) for i in key]
            return ''.join(chr(a^b) for a, b in zip(text_shifr, key_shifr))

In [3]: text = 'С Новым Годом, друзья!'
        key = generate_key (len(text))
        shifr = gamming (text, key)
        print ('Шифротекст: ', shifr)

        Шифротекст:  ыІЮЎVе№€RyoËЏv Wë€Ї¤Уmu

In [4]: gamming(gamming (text, key), key)

Out[4]: 'С Новым Годом, друзья!'
```

рис.1. Программа.

2. Подоберём ключ, чтобы получить один из вариантов прочтения открытого текста. (рис.2).

```
In [3]: text = 'С Новым Годом, друзья!'
        key = generate_key (len(text))
        shifr = gamming (text, key)
        print ('Шифротекст: ', shifr)

        Шифротекст:  ыІЮЎVе№€RyoËЏv Wë€Ї¤Уmu

In [4]: gamming(gamming (text, key), key)

Out[4]: 'С Новым Годом, друзья!'

In [5]: key_2 = generate_key (len(text))
        text_2 = gamming (shifr, key_2)
        print ('Расшифрованный текст: ', text_2)

        Расшифрованный текст:  ӨЂ¾лЙЄг КИиЎа□□ГтЎШВs6
```

рис.2. Определение ключа.

3. Контрольные вопросы:

1) Поясните смысл однократного гаммирования. Каждый символ открытого текста попарно по модулю 2 складывается с символом ключа.
2) Перечислите недостатки однократного гаммирования. Ключ нельзя переиспользовать. Размер ключа должен быть такой же, как и размер текста.
3) Перечислите преимущества однократного гаммирования. Основные преимущества однократного гаммирования – это симметричность и криптостойкость. Также простота использования.
4) Почему длина открытого текста должна совпадать с длиной ключа? Потому что каждый символ открытого текста должен складываться символом ключа попарно.

5) Какая операция используется в режиме однократного гаммирования, назовите её особенности? В режиме однократного гаммирования используется сложение по модулю 2. Её особенность состоит в том, что она симметрична, то есть при повторном применении дает исходное значение. Например, если мы применим к открытому тексту гаммирование, а затем к получившемуся зашифрованному тексту применим гаммирование еще раз с темже ключом, то получим изначальный открытый текст.
6) Как по открытому тексту и ключу получить шифротекст? Нужно попарно сложить по модулю 2 символы текста с символами ключа.
7) Как по открытому тексту и шифротексту получить ключ? Нужно попарно сложить по модулю 2 символы открытого текста с символами шифротекста.
8) В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра? Необходимые и достаточные условия абсолютной стойкости шифра: а) полная случайность ключа; б) равенство длин ключа и открытого текста; в) использование ключа однкратно.

Выводы

Я приобрела практические навыки применения режима однократного гаммирования.