Отчет по лабораторной работе номер 7

Хамбалеев Булат Галимович

Содержание

List of Tables

List of Figures

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Задание

Лабораторная работа подразумевает использование языков программирования для создания программы для щифрования и дещифрования в режиме однократного гаммирования.

3 Теория

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных.

4 Выполнение работы

1. Разработаетм приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.(рис 1-2)

Ввод [1]:
```
import random
```

Ввод [2]:
```
import string
```

Ввод [3]:
```
word = ("С Новым Годом, друзья!")
```

Ввод [4]:
```
def key_generator(size=6, chars = string.ascii_letters +string.digits):
    return ''.join(random.choice(chars) for _ in range(size))
def change(s):
    return ":".join("{:02x}".format(ord(c)) for c in s)
```

Ввод [5]:
```
key = key_generator(len(word))
```

Ввод [6]:
```
print(f'Ключ в строчном виде: {key}')
```

```
Ключ в строчном виде: QbWnd43zcct5V4FSa2qXlD
```

Ввод [13]:
```
def gammirovanie(word,key):
    word_ascii = [ord(i) for i in word]
    key_ascii = [ord(i) for i in key]
    enc_str = ''.join(chr(s ^ k) for s, k in zip(word_ascii, key_ascii))
    return enc_str
```

Ввод [15]:
```
def true_key_find(word,enc_str):
    sm_ascii = [ord(i) for i in word]
    enc_str_ascii = [ord(i) for i in enc_str]
    true_key = ''.join(chr(s ^ k) for s,k in zip(enc_str_ascii,sm_ascii))
    return true_key
```

Ввод [11]:
```
def unencrypt(enc_str, key):
    enc_str_ascii = [ord(i) for i in enc_str]
    key_ascii = [ord(i) for i in key]
    true_str = ''.join(chr(s ^ k) for s,k in zip(enc_str_ascii, key_ascii))
    return true_str
```

Figure 4.1: рис.1. Программа, часть 1.

```
Ввод [14]: enc_str=gammirovanie(word,key)

Ввод [16]: new_key=key_generator(len(enc_str))
           unencrypted_new_key = unencrypt(enc_str, new_key)
           true_key = true_key_find(word,enc_str)
           unencrypted_true_key = unencrypt(enc_str, true_key)

Ввод [17]: print(f'Закодированная строка: {enc_str}')

           Закодированная строка: ΨВъèiѾЏZΨйрЋѪ?fʌСцЦДУе

Ввод [20]: print(f'В шестнадцатеричной системе:{change(enc_str)}')

           В шестнадцатеричной системе:470:42:44a:450:456:47f:40f:5a:470:45d:440:40b:46a:18:66:467:421:471:446:414:423:65

Ввод [21]: print(f'Подобранный ключ: {new_key}')

           Подобранный ключ: glXQrc7xgVz8tQgBQBypuS

Ввод [22]: print(f'Расшифрованная ключом строка: {unencrypted_new_key}')

           Расшифрованная ключом строка: 3.ВЁФМи"3ЋкгOI?XΨгпѤi6

Ввод [24]: print(f'Настоящий ключ: {true_key}')

           Настоящий ключ: QbWnd43zcct5V4FSa2qXlD

Ввод [25]: print(f'Декодированная строка: {unencrypted_true_key}')

           Декодированная строка: С Новым Годом, друзья!

Ввод [ ]:
```

Figure 4.2: рис.2. Программа, часть 2.

5 Контрольные вопросы

1. Поясните смысл однократного гаммирования.

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, то есть последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Однократное гаммирование – это когда каждый символ попарно с символом ключа складываются по модулю 2 (XOR).

2. Перечислите недостатки однократного гаммирования.

Размер ключевого материала должен совпадать с размером передаваемых сообщений. Также необходимо иметь эффективные процедуры для выработки случайных равновероятных двоичных последовательностей и специальную службу для развоза огромного количества ключей. А ещё, если одну и ту же гамму использовать дважды для разных сообщений, то шифр из совершенно стойкого превращается в «совершенно нестойкий» и допускает дешифрование практически вручную.

3. Перечислите преимущества однократного гаммирования.

С точки зрения теории криптоанализа метод шифрования случайной однократной равновероятной гаммой той же длины, что и открытый текст, является невскрываемым. Кроме того, даже раскрыв часть сообщения, дешифровщик не сможет хоть сколько-нибудь поправить положение -

информация о вскрытом участке гаммы не дает информации об остальных ее частях. К достоинствам также можно отнести простоту реализации и удобство применения.

4. Почему длина открытого текста должна совпадать с длиной ключа?

Потому что каждый символ открытого текста должен складываться с символом ключа попарно.

5. Какая операция используется в режиме однократного гаммирования, назовите её особенности?

В режиме однократного гаммирования используется сложение по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста. Особенность заключается в том, что этот алгоритм шифрования является симметричным. Поскольку двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, шифрование и расшифрование выполняется одной и той же программой.

6 Библиография

1. ТУИС РУДН

2. Статья на сайте “https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BC%D0%BC%D0%B8

7 Выводы

Во время выполнения лабораторной работы я освоил на практике применение режима однократного гаммирования.