Отчет по лабораторной работе №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Бармина Ольга Константиновна

2022 Sep 21th

Содержание

Список таблиц

Список иллюстраций

1. Цель работы

Целью данной работы является освоение на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом. [1]

2. Выполнение лабораторной работы

1. Подгрузила необходимые библиотеки, задала функцию для генерации ключа, преобразованию ключа в шестнадцатеричное предствление, и для шифрования текста.

```
import string
import random
```

```
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(text1, text2):
    t1 = [ord(i) for i in text1]
    t2 = [ord(i) for i in text2]
    return ''.join(chr(a^b) for a,b in zip(t1, t2))
```

Рис. 2.1.: рис 1. функции

2. Задала 2 текста, создала ключ, преобразовала его в шестнадцатеричное представление.

```
p1 = "НаВашисходящийот1204"
p2 = "ВСеверныйфилиалБанка"

key = f2(len(p1))
key
```

```
'i W P V 1 n o k 7 f p e u J Z r 4 r l 6'
```

```
hex_key = f1(key)
hex_key
```

```
'69 20 57 20 50 20 56 20 31 20 6e 20 6f 20 6b 20 37 20 66 20 70 20 65 20 75 20 4a 20 5a 20 72 20 34 20 72 20 6c 20 36'
```

Рис. 2.2.: рис 2. создание ключа

3. Закодировала оба сообщения с помощью ключа. Создала декриптор, использующий оба сообщения. Раскодировала сообщения при помощи него.

```
ecr1 = f3(p1, key)
ecr2 = f3(p2, key)
ecr1, ecr2
```

```
('VAxAИИЗюЦДСмїЙsЪ\x06\x12V\x14', 'ОЁЪВюЏЖЖЈЮiЛїAѣбЇНќA')
```

```
decr = f3(ecr1, ecr1)
f3(decr, p1), f3(decr, p2)
```

```
('НаВашисходящийот1204', 'ВСеверныйфилиалБанка')
```

Рис. 2.3.: рис 3. шифрование

3. Контрольные вопросы

1. Чтобы определить один из текстов, зная другой, необходимо вопсользоваться следующей формулой: $C_1 \oplus C_2 \oplus + P_1 = P_1 \oplus P_2 \oplus + P_1 = P_2$, где C_1 и C_2 - шифротексты. Т.е. ключ в данной формуле не используется.

2. При повторном использовании ключа при шифровании текста получим исходное сообщение.

3. Режим шифрования однократного гаммирования одним ключом двух открытых текстов реализуется по следующей формуле:

$$C_1 = P_1 \oplus + K$$

$$C_2 = P_2 \oplus + K,$$

   где C_i - шифротексты, P_i - открытые тексты, K - единый ключ шифровки

4. Недостатки шифрования одним ключом двух открытых текстов: Во-первых, имея на руках одно из сообщений в открытом виде и оба шифротекста, злоумышленник способен расшифровать каждое сообщение, не зная ключа. Во-вторых, зная шаблон сообщений, злоумышленник получает возможность определить те символы сообщения P_2, которые находятся на позициях известного шаблона сообщения P_1.

5. Преимущества шифрования одним ключом двух открытых текстов: Такой подход помогает упростить процесс шифрования и дешифровки. Также,

при отправке сообщений между 2-я компьютерами, удобнее пользоваться одним общим ключом для передаваемых данных

4. Выводы

В ходе работы мы освоили на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

5. Список литературы

1. Методические материалы курса