Лабораторная работа №8

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

Якушевич Артём Юрьевич

Содержание

1 Цель работы **5**

2 Задание **6**

3 Выполнение лабораторной работы **7**

4 Выводы **9**

5 Ответы на контрольные вопросы **10**

6 Список литературы **12**

Список иллюстраций

3.1 Функция, шифрующая данные 7
3.2 Результат работы функции, шифрующей данные 8
3.3 Функция, дешифрующая данные 8

Список таблиц

1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом [1].

2 Задание

1. Написать программу, которая должна определять вид шифротекстов при известных открытых текстах и при известном ключе.
2. Также эта программа должна определить вид одного из текстов, зная вид другого открытого текста и зашифрованный вид обоих текстов (т.е. не нужно использовать ключ при дешифровке).

3 Выполнение лабораторной работы

1. Написал функцию шифрования, которая определяет вид шифротекста при известном ключе и известных открытых текстах “НаВашисходящийот1204” и “ВСеверныйфилиалБанка”. Ниже представлены функция, шифрующая данные (рис - @fig:001), а также работа данной функции (рис - @fig:002).

```
p1 = "НаВашисходящийот1204"
p2 = "ВСеверныйфилиалБанка"
key, res1, res2 = encryption(p1, p2)
```

```
Открытый 1ый текст:  НаВашисходящийот1204

Открый 1ый текст в шестнадцатеричном представлении:  cd e0 c2 e0 f8 e8 f1 f5 ee e4 ff f9 e8 e9 ee f2 31 32 30 34

Открытый 2ой текст:  ВСеверныйфилиалБанка

Открый 2ой текст в шестнадцатеричном представлении:  c2 d1 e5 e2 e5 f0 ed fb e9 f4 e8 eb e8 e0 eb c1 e0 ed ea e0

Ключ в шестнадцатеричном представлении:  8 c2 7c 9a b1 23 e5 53 26 90 3 5b ce e9 e7 c7 e4 5c 81 4f

Зашифрованный 1ый текст в шестндцатеричном представлении:  c5 22 be 7a 49 cb 14 a6 c8 74 fc a2 26 00 09 35 d5 6e b1 7b

Зашифрованный 2ой текст в шестндцатеричном представлении:  ca 13 99 78 54 d3 08 a8 cf 64 eb b0 26 09 0c 06 04 b1 6b af

Зашифрованный 1ый текст:  E"szIЛ¦Итьў& 5Xn±{

Зашифрованный 2ой текст:  K™xTЁПdл°&   ±kI
```

Рис. 3.1: Функция, шифрующая данные

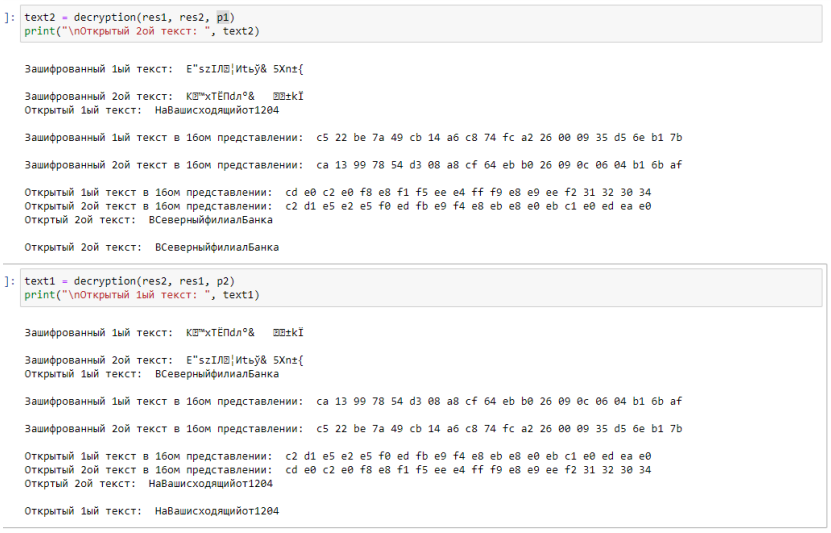

Рис. 3.2: Результат работы функции, шифрующей данные

2. Написал функцию дешифровки, которая определяет вид одного из текстов, зная вид другого открытого текста и зашифрованный вид обоих текстов (т.е. не использует ключ). (рис - @fig:003). А также представил результаты работы программы (рис - @fig:004).

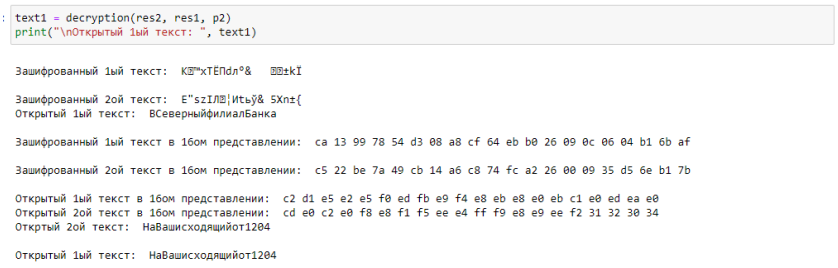

Рис. 3.3: Функция, дешифрующая данные

Результат работы функции, дешифрующей данные

4 Выводы

Освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

5 Ответы на 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

6 Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом.