Лабораторная работа №8

Якушевич Артём Юрьевич - студент группы НКНбд-01-18

16.12.2021

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

Прагматика выполнения

- Криптография - наука о методах шифрования. Умение шифровать различные исходные тексты одним ключом является необходимым для дальнейшего знакомства с криптографией.

Цель выполнения лабораторной работы

- Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

Задачи выолнения работы

- Написать программу, которая должна определять вид шифротекстов при известных открытых текстах и при известном ключе.
- 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).

Результаты выполнения лабораторной работы

- 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°&   ±kЇ
```

Рис. 1: Функция, шифрующая данные

```
]: text2 = decryption(res1, res2, p1)
   print("\nОткрытый 2ой текст: ", text2)

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

   Зашифрованный 2ой текст:  K¤™xTËПdл°&   ¤¤±kЇ
   Открытый 1ый текст:  НаВашисходящийот1204

   Зашифрованный 1ый текст в 16ом 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 16ом представлении:  ca 13 99 78 54 d3 08 a8 cf 64 eb b0 26 09 0c 06 04 b1 6b af

   Открытый 1ый текст в 16ом представлении:  cd e0 c2 e0 f8 e8 f1 f5 ee e4 ff f9 e8 e9 ee f2 31 32 30 34
   Открытый 2ой текст в 16ом представлении:  c2 d1 e5 e2 e5 f0 ed fb e9 f4 e8 eb e8 e0 eb c1 e0 ed ea e0
   Откртый 2ой текст:  ВСеверныйфилиалБанка

   Открытый 2ой текст:  ВСеверныйфилиалБанка

]: text1 = decryption(res2, res1, p2)
   print("\nОткрытый 1ый текст: ", text1)

   Зашифрованный 1ый текст:  K¤™xTËПdл°&   ¤¤±kЇ

   Зашифрованный 2ой текст:  E"szIЛ¤¦Итьў& 5Xn±{
   Открытый 1ый текст:  ВСеверныйфилиалБанка

   Зашифрованный 1ый текст в 16ом представлении:  ca 13 99 78 54 d3 08 a8 cf 64 eb b0 26 09 0c 06 04 b1 6b af

   Зашифрованный 2ой текст в 16ом представлении:  c5 22 be 7a 49 cb 14 a6 c8 74 fc a2 26 00 09 35 d5 6e b1 7b

   Открытый 1ый текст в 16ом представлении:  c2 d1 e5 e2 e5 f0 ed fb e9 f4 e8 eb e8 e0 eb c1 e0 ed ea e0
   Открытый 2ой текст в 16ом представлении:  cd e0 c2 e0 f8 e8 f1 f5 ee e4 ff f9 e8 e9 ee f2 31 32 30 34
   Откртый 2ой текст:  НаВашисходящийот1204

   Открытый 1ый текст:  НаВашисходящийот1204
```

Рис. 2: Результат работы функции, шифрующей данные

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

```
text1 = decryption(res2, res1, p2)
print("\nОткрытый 1ый текст: ", text1)
```

```
Зашифрованный 1ый текст:  K□™xTËПdл°&   □□±kЇ

Зашифрованный 2ой текст:  E"szIЛ□¦Итьў& 5Xn±{
Открытый 1ый текст:  ВСеверныйфилиалБанка

Зашифрованный 1ый текст в 16ом представлении:  ca 13 99 78 54 d3 08 a8 cf 64 eb b0 26 09 0c 06 04 b1 6b af

Зашифрованный 2ой текст в 16ом представлении:  c5 22 be 7a 49 cb 14 a6 c8 74 fc a2 26 00 09 35 d5 6e b1 7b

Открытый 1ый текст в 16ом представлении:  c2 d1 e5 e2 e5 f0 ed fb e9 f4 e8 eb e8 e0 eb c1 e0 ed ea e0
Открытый 2ой текст в 16ом представлении:  cd e0 c2 e0 f8 e8 f1 f5 ee e4 ff f9 e8 e9 ee f2 31 32 30 34
Откртый 2ой текст:  НаВашисходящийот1204

Открытый 1ый текст:  НаВашисходящийот1204
```

Рис. 3: Функция, дешифрующая данные

Результат работы функции, дешифрующей данные

Таким образом, я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.