Лабораторная работа №8

Филиппова Вероника Сергеевна- студентка группы НКНбд-01-18

17.12.2021

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

Цель выполнения лабораторной работы

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

Задачи выполнения работы

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).

Результаты выполнения лабораторной работы. Часть 1

Написала функцию шифрования, которая определяет вид шифротекста при известном ключе и известных открытых текстах "НаВашисходящийот1204" и "ВСеверныйфилиалБанка".

Ввод [12]:
```
import numpy as np
```

Ввод [13]:
```
def encryption(text1, text2):
    print("Открытый текст №1: ", text1)
    # Массив из символов открытого 1го текста в 16 системе:
    text_array1 = []
    for i in text1:
        text_array1.append(i.encode("cp1251").hex())
    print("\nОткрый  текст в 16 системе: ", *text_array1)

    print("\nОткрытый текст №2: ", text2)
    # Задам массив из символов открытого 2го текста в 16 системе:
    text_array2 = []
    for i in text2:
        text_array2.append(i.encode("cp1251").hex())
    print("\nОткрый текст №2 в 16 системе: ", *text_array2)

    # Задам случайно сгенерированный ключ в 16 системе:
    key_dec = np.random.randint(0, 255, len(text1))
    key_hex = [hex(i)[2:] for i in key_dec]
    print("\nКлюч в 16 системе: ", *key_hex)

    # Задам зашифрованный 1ый текст в 16 системе:
    crypt_text1 = []
    for i in range(len(text_array1)):
        crypt_text1.append("{:02x}".format(int(text_array1[i], 16) ^ int(key_hex[i], 16)))
    print("\nЗашифрованный текст №1 в 16 системе: ", *crypt_text1)

    # Задам зашифрованный 2ой текст в 16 системе:
    crypt_text2 = []
    for i in range(len(text_array2)):
        crypt_text2.append("{:02x}".format(int(text_array2[i], 16) ^ int(key_hex[i], 16)))
    print("\nЗашифрованный текст №2 в 16 системе: ", *crypt_text2)

    # Задам зашифрованный 1ый текст :
    final_text1 = bytearray.fromhex("".join(crypt_text1)).decode("cp1251")
    print("\nЗашифрованный текст №1: ", final_text1)

    # Задам зашифрованный 2ой текст :
    final_text2 = bytearray.fromhex("".join(crypt_text2)).decode("cp1251")
    print("\nЗашифрованный текст №2: ", final_text2)

    return key_hex, final_text1, final_text2
```

Результаты выполнения лабораторной работы. Часть 2

Написала функцию дешифровки, которая определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Ввод [14]:
```
def decryption(cr_text1, cr_text2, op_text1):
    print("\nЗашифрованный текст №1 : ", cr_text1)
    print("\nЗашифрованный текст №2: ", cr_text2)
    print("Открытый текст №1: ", op_text1)

    cr_text_hex1 = []
    for i in cr_text1:
        cr_text_hex1.append(i.encode("cp1251").hex())
    print("\nЗашифрованный текст №1 в 16 системе: ", *cr_text_hex1)

    cr_text_hex2 = []
    for i in cr_text2:
        cr_text_hex2.append(i.encode("cp1251").hex())
    print("\nЗашифрованный текст №2 в 16 системе: ", *cr_text_hex2)

    op_text_hex1 = []
    for i in op_text1:
        op_text_hex1.append(i.encode("cp1251").hex())
    print("\nОткрытый текст №1 в 16 системе: ", *op_text_hex1)

    cr1_cr2 = []
    op_text_hex2 = []
    for i in range(len(op_text1)):
        cr1_cr2.append("{:02x}".format(int(cr_text_hex1[i],16) ^ int(cr_text_hex2[i],16)))
        op_text_hex2.append("{:02x}".format(int(cr1_cr2[i], 16) ^ int(op_text_hex1[i], 16)))

    print("Открытый текст №2 в 16 системе: ", *op_text_hex2)
    op_text2 = bytearray.fromhex("".join(op_text_hex2)).decode("cp1251")
    print("Открытый текст№2: ", op_text2)
    return op_text2
```

Ввод [18]:
```
text1 = decryption(res2, res1, p2)
print("\nОткрытый текст №1: ", text1)
```

```
Зашифрованный текст №1 :  c{O5>D,bYt6ЗAreВЗЗqQ

Зашифрованный текст №2:  юJh7†\0T◆duZASi·AZ»…
Открытый текст №1:  ВСеверныйфилиалБанка

Зашифрованный текст №1 в 16 системе:  f1 7b 4f 35 9b 44 2c dc d3 74 e1 06 c0 b4 b8 1e 11 de 71 51

Зашифрованный текст №2 в 16 системе:  fe 4a 68 37 86 5c 30 d2 d4 64 f6 14 c0 bd bf 2d c0 01 ab 85

Открытый текст №1 в 16 системе:  c2 d1 e5 e2 e5 f0 ed fb e9 f4 e8 eb e8 e0 eb c1 e0 ed ea e0
Открытый текст №2 в 16 системе:  cd e0 c2 e0 f8 e8 f1 f5 ee e4 ff f9 e8 e9 ee f2 31 32 30 34
Открытый текст№2:  НаВашисходящийот1204

Открытый текст №1:  НаВашисходящийот1204
```

Выводы

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