Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Липатникова М.С. группа НФИбд-02-19

Содержание

List of Figures

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Выполнение лабораторной работы

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение (fig. 2.1), позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно: 1. Определить вид шифротекста при известном ключе и известном откры- том тексте. 2. Определить ключ, с помощью которого шифротекст может быть преоб- разован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Создала 4 функции: - одна генерирует ключ из ASCII-кодов по количеству букв в сообщении; - вторая делает шифрование в режиме однократного гаммирования: сначала каждая буква текста и ключа изменяется на число из таблицы символов Unicode, представляющее его позицию, потом это число переводится в 16-ную систему. Далее текст возводится в степень ключа - это зашифрованное сообщение; - в третьей функции мы можем найти открытый ключ по тексту и зашифрованному тексту; - в четвертой функции находим открытое собщение из зашифрованного и ключа.

```
Ввод [1]:  import random
           import string
```

```
Ввод [2]:  def key_gen(text):
               simb = string.ascii_letters + string.digits
               return ''.join(random.choice(simb) for i in range(len(text)))
           def gamm(text, key):
               text_cypher = [hex(ord(i))[2:] for i in text]
               key_cypher = [hex(ord(i))[2:] for i in key]
               print("Текст в 16-ной системе: ", text_cypher, '\nКлюч в 16-ной системе: ', key_cypher)
               return ''.join(chr(int(a, 16)^int(b, 16)) for a,b in zip (text_cypher, key_cypher))
```

```
Ввод [3]:  text = "С Новым Годом, друзья!"
           key = key_gen(text)
           cypher = gamm(text, key)
           print("Зашифрованный текст: ", cypher,'\nКлюч: ', key)

           Текст в 16-ной системе:  ['421', '20', '41d', '43e', '432', '44b', '43c', '20', '413', '43e', '434', '43e', '43c', '2c', '20
           ', '434', '440', '443', '437', '44c', '44f', '21']
           Ключ в 16-ной системе:  ['48', '4a', '6f', '4c', '70', '4a', '66', '4b', '45', '66', '4a', '54', '4a', '51', '68', '67', '7a
           ', '69', '71', '35', '42', '48']
           Зашифрованный текст:  ѩjѲѲтЁњkіјѾѪѶ}HѓкЪцѹЍi
           Ключ:  HJoLpJfKEfJTJQhgziq5BH
```

```
Ввод [4]:  def key_f(text, text_c):
               text1 = [hex(ord(i))[2:] for i in text]
               text_c1 = [hex(ord(i))[2:] for i in text_c]
               return ''.join(chr(int(a,16)^int(b,16)) for a,b in zip (text1, text_c1))
```

```
Ввод [5]:  print("Ключ был: ",key_f(text,cypher))

           Ключ был:  HJoLpJfKEfJTJQhgziq5BH
```

```
Ввод [6]:  def text_f(cypher, key):
               cypher1 = [hex(ord(i))[2:] for i in cypher]
               key1 = [hex(ord(i))[2:] for i in key]
               return ''.join(chr(int(a,16)^int(b,16)) for a,b in zip (cypher1, key1))
```

```
Ввод [7]:  print("Текст был: ", text_f(cypher,key))

           Текст был:  С Новым Годом, друзья!
```

Figure 2.1: Программа

3 Вывод

Освоила на практике применение режима однократного гаммирования.

4 Список литературы

1. Теоретические материалы курса.