Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Кувшинова Ксения Олеговна[1]

21.10.2022, Moscow

[1]RUDN University, Moscow, Russian Federation

Цель работы

Целью данной лабораторной работы является освоить на практике применение режима однократного гаммирования.

Указание к работе

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Наложение гаммы представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ⊕) между элементами гаммы и элементами подлежащего сокрытию текста.

Задание к лабораторной работе

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

Выполнение лабораторной работы

Импортируем необходимые для работы библиотеки (fig. 1)

```
[1]  import string
     import random
```

Figure 1: Импорт библиотек

Выполнение лабораторной работы

Напишем функции формирования ключа, перевода данных в 16 систему и шифрования текста. (fig. 2)

```
#формирование ключа
def key(size):
  #генерируем ключ
  key1 = ''.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))
  print("Key: ", key1)
  #переводим в 16 СИ
  key2 = coding(key1)
  print("Key in 16: ", key2)
  return key2

#функция перевода в 16 СИ
def coding(smth):
  smth1 = ' '.join(hex(ord(i))[2:] for i in smth)
  return smth1

#шифрование
def crypt(text, key):
  t = [ord(i) for i in text]
  k = [ord(j) for j in key]
  sixt_t=''.join(chr(i^j) for i,j in zip(t,k))
  return sixt_t
```

Figure 2: Функции формирования ключа, перевода данных в 16 систему и шифрования

Выполнение лабораторной работы

Зашифруем и дешифруем предложенный текст с помощью сгенерированного ключа. (fig. 3)

```
[12] mg = "С Новым Годом, друзья!"
     print("Text: ", mg)
     key = key(len(mg))
     crypt1 = crypt(mg,key)
     print("Зашифрованный текст:", crypt1)
     crypt16 = coding(crypt1)
     print("Зашифрованный текст в 16:", crypt16)
     decrypt = crypt(crypt1, key)
     print("Расшифрованный текст:", decrypt)

     Text:  С Новым Годом, друзья!
     Key:  z88vCQhHvPygeVwMx9wmac
     Key in 16:  7a 38 38 76 43 51 68 48 76 50 79 67 65 56 77 4d 78 39 77 6d 61 63
     Зашифрованный текст: ЖАнЙЊжЏ□гЉЂОЈ□□ЁфЂЁV₃□
     Зашифрованный текст в 16: 416 41 43d 40d 40a 46b 40f 18 433 409 402 41e 408 1f 0 401 471 463 401 474 46f 15
     Расшифрованный текст: С Новым Годом, друзья!
```

Figure 3: Шифрование и дешифрование текста

Выполнение лабораторной работы

Определим ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. (fig. 4)

```
[13] key3 = crypt(mg, crypt1)
     dec_key = crypt(crypt1, key3)
     print("New Key: ", key3)
     print("Проверка: ", dec_key )

     New Key:  7a 38 38 76 43 51 68 4
     Проверка:  С Новым Годом, друзья!
```

Figure 4: Шифрование и дешифрование текста

Результат выполнения работы

В ходе выполнения лабораторной работы мы освоили на практике применение режима однократного гаммирования.

Библиография

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Элементы криптографии. Однократное гаммирование [Текст] / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 3 с. [^1]: Элементы криптографии. Однократное гаммирование.