Лабораторная работа №8

Лукьянова Ирина Владимировна

10 October 2022

RUDN University, Moscow, Russian Federation

Цель лабораторной работы

Цель лабораторной работы

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

Задачи выполнения лабораторной работы

Задачи выполнения лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Выполнение лабораторной работы

Выполнение лабораторной работы

Добавляем необходимые библиотеки и создаем функцию генерации ключа. Затем создаем функцию перевода в 16 строку и переводим ключ, с помощью этой функции(рис. 1)

```
[2]: import random
     import string
     import numpy as np

[3]: P1 = 'НаВашисходящийот1204'
     P2 = 'ВСеверныйфилиалБанка'

[4]: def f1(n): #генерация ключа
         k = []
         for i in range(n):
             k.append(random.choice(string.ascii_letters + string.digits))
         return k

[6]: key = f1(len(P1))
     np.array(key)

[6]: array(['y', 'h', 'H', '0', 'E', 'u', 'q', '3', 'a', 'h', '7', 'F', 'p',
            'P', 'v', 'r', 'U', 'K', 't', 'E'], dtype='<U1')

[7]: def f2(t): #перевод в 16 строку
         a = []
         for i in t:
             a.append(hex(ord(i))[2:])
         return a

[8]: key16 = f2(key)
     np.array(key16)

[8]: array(['79', '68', '48', '30', '45', '75', '71', '33', '61', '68', '37',
            '46', '70', '50', '76', '72', '55', '4b', '74', '45'], dtype='<U2')
```

Figure 1: Код

Выполнение лабораторной работы

Выполнение лабораторной работы

Создаем функцию сложения по модулю 2 (XOR) для нее нам нужна еще одна функция, которая переводит наши символы в числа.(рис. 2)

```
[9]: def f3(t,k): #XOR
         a = []
         for (i,j) in zip(t,k):
             a.append(chr(i^j))
         return a

     def for16(a): #превращаем символы в числа
         f = []
         for i in a:
             f.append(ord(i))
         return f

[10]: C1 = f3(for16(P1), for16(key))
      np.array(C1)

[10]: array(['Ѥ', 'j', 'ћ', 'È', 'Й', 'э', 'a', 'Ў', 'ѵ', 'ќ', 'Оу', 'Ц', 'ш',
             'ѩ', 'ш', 'a', 'd', 'y', 'D', 'q'], dtype='<U1')

[11]: C2 = f3(for16(P2), for16(key))
      np.array(C2)

[11]: array(['ѫ', 'щ', 'ѡ', 'Ђ', 'Ѱ', 'e', 'ь', 'Оу', 'j', 'Ь', 'Ц', 'ѡ', 'ш',
             'Ш', 'э', 'Ъ', 'ѥ', 'Ў', 'ю', 'v'], dtype='<U1')
```

Figure 2: Код 2

Выполнение лабораторной работы

Выполнение лабораторной работы

В итоге получаем следующие данные: (рис. 3)

```
[13]: print("Открытый текст:\nP1 = ", P1, "\nP2 = ", P2)
      print("Ключ: ", ''.join(key))
      print("Ключ в 16: ", ' '.join(key16))
      print("Шифр:\nC1 = ", ''.join(C1), "\nC2 = ", ''.join(C2))

      Открытый текст:
      P1 =  НаВашисходящийот1204
      P2 =  ВСеверныйфилиалБанка
      Ключ:  yhH0Euq3ah7FpPvrUKtE
      Ключ в 16:  79 68 48 30 45 75 71 33 61 68 37 46 70 50 76 72 55 4b 74 45
      Шифр:
      C1 =  ЄjњЀЙэаЎцќОуЏшњшadyDq
      C2 =  ѫщѿЂѰеьОуjЬЏѿшШэЂќЎюv
```

Figure 3: Вывод данных

Далее мы используем сложение по модулю 2 между шифротекстами, после повторяем операцию с одним из открытых текстов. В итоге получаем второй расшифрованный текст. Данные операции также действуют и для второго текста, что я и демонстрирую на следующем слайде.

Выполнение лабораторной работы

Выполнение лабораторной работы

Мы используем уже написанные функции для того, чтобы расшифровать текст без ключа: (рис. 4)

```
[14]: C = f3(for16(C1), for16(C2))
      np.array(C2)

[14]: array(['ѫ', 'щ', 'ѡ', 'Ђ', 'Ѱ', 'е', 'ь', 'Оу', 'j', 'Ь', 'Ц', 'ѡ', 'ш',
             'Ш', 'э', 'Ъ', 'ѥ', 'Ѵ', 'ю', 'v'], dtype='<U1')

[15]: p_1 = f3(for16(C), for16(P2))
      np.array(p_1)

[15]: array(['Н', 'а', 'В', 'а', 'ш', 'и', 'с', 'х', 'о', 'д', 'я', 'щ', 'и',
             'й', 'о', 'т', '1', '2', '0', '4'], dtype='<U1')

[16]: p_2 = f3(for16(C), for16(P1))
      np.array(p_2)

[16]: array(['В', 'С', 'е', 'в', 'е', 'р', 'н', 'ы', 'й', 'ф', 'и', 'л', 'и',
             'а', 'л', 'Б', 'а', 'н', 'к', 'а'], dtype='<U1')

[17]: print("C1 XOR C2: ", ''.join(C))
      print("P1 = C1 XOR C2 XOR P2: ", ''.join(p_1))
      print("P2 = C1 XOR C2 XOR P1: ", ''.join(p_2))

      C1 XOR C2:  '}x|pwr     SЁЦЊЄ
      P1 = C1 XOR C2 XOR P2:  НаВашисходящийот1204
      P2 = C1 XOR C2 XOR P1:  ВСеверныйфилиалБанка
```

Figure 4: Вывод данных

Результаты выполнения лабораторной работы

Результаты выполнения лабораторной работы

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.