Лабораторная работа №8

Алескеров Тимур

Декабрь, 2021 Москва

RUDN University, Moscow, Russian Federation

Прагматика выполнения лабораторной работы

Прагматика выполнения лабораторной работы

Проблемой защиты информации при ее передаче между абонентами люди занимаются на протяжении всей своей истории. Человечеством изобретено множество способов, позволяющих в той или иной мере скрыть смысл передаваемых сообщений от противника. В этой лабораторнй работе мы изучили один из методов шифрования - метод однократного гаммирования.

Цель работы

Цель работы

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

Задачи

Задачи

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

Результат

Программа шифрования

Ввод [4]:
```
import random as rnd
import string as strg

abc = strg.ascii_letters.join(strg.digits)
abc
```

Out[4]:
```
'0abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ2abcdefghi
jklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ3abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ4abcdefghijklmnopqrst
uvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ5abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ6abcdefghijklmnopqrstuvwxyzABCDE
FGHIJKLMNOPQRSTUVWXYZ7abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ8abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOP
QRSTUVWXYZ9'
```

Ввод [6]:
```
p1 = "НаВашисходящийот1204"
p2 = "ВСеверныйфилиалБанка"

k = "".join(rnd.choice(abc) for i in range(len(p1)))
```

Ввод [8]:
```
def xor_string(data, key):
    return "".join(chr(ord(x)^ord(y)) for x, y in zip(data, key))
```

Ввод [9]:
```
c1 = xor_string(p1, k)

bytes(c1, "UTF-8").hex()
```

Out[9]:
```
'd1a5d1bad1a8d1a5d0acd19dd084d0a2d1bdd1a7d09cd0aad19dd1a3d19fd0965a7c5d42'
```

Рис. 1: Листинг программы

Программа шифрования

```
Ввод [8]:
def xor_string(data, key):
    return "".join(chr(ord(x)^ord(y)) for x, y in zip(data, key))

Ввод [9]:
c1 = xor_string(p1, k)

bytes(c1, "UTF-8").hex()

Out[9]: 'd1a5d1bad1a8d1a5d0acd19dd084d0a2d1bdd1a7d09cd0aad19dd1a3d19fd0965a7c5d42'

Ввод [11]:
c2 = xor_string(p2, k)

bytes(c2, "UTF-8").hex()

Out[11]: 'd1aad1abd18fd1a7d191d0a5d1b8d0acd1bad097d1abd198d19dd1aad19ad185d19bd1b3d197d186'

Ввод [12]:
p1_xor_p2 = xor_string(p1, p2)

bytes(p1_xor_p2, "UTF-8").hex()

Out[12]: '0f1127027d787c0e0770777200090553d081d08fd08ad084'

Ввод [14]:
p2_found = xor_string(p1_xor_p2, p1)
p2_found

Out[14]: 'ВСеверныйфилиалБанка'

Ввод [16]:
p2_found == p2

Out[16]: True
```

Рис. 2: Листинг программы 2

Программа шифрования

```
Out[16]: True

Ввод [18]: p1_found = xor_string(p1_xor_p2, p2_found)
           p1_found

Out[18]: 'НаВашисходящийот1204'

Ввод [19]: p1_found == p1

Out[19]: True
```

Рис. 3: Листинг программы 3

Вывод

В ходе данной лабораторной работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом, разработал приложение, позволяющие шифровать и дешифровать различные тексты в режиме однократного гаммирования.

Спасибо за внимание!