Презентация лабораторной работы 8

ТЕМА «**Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом**»

Выполнил:
Студент группы НПИбд-02-21
Студенческий билет № 1032205421
Стелина Петрити

Цель работы

Ознакомиться с практическим использованием метода одноразового шифрования с помощью гаммирования, закодировав несколько исходных текстов с использованием одного ключа.

Последовательность выполнения работы

1. 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.Определить вид шифротекста при известном ключе и известном открытом тексте.

   Задача состоит в том, чтобы разработать приложение, которое будет шифровать и дешифровать тексты с использованием однократного гаммирования, а затем попытаться прочитать тексты без знания ключа.

```
def xorbytes(data, key):
  extend_key = (key * (len(data)//len(key)+1))[:len(data)]
  return bytes ([b1^b2 for b1, b2, in zip (data, extend_key)])

def decryption (cipher_txt, key):
  return xorbytes(cipher_txt , key).decode('utf-8')

key=bytes([0x05, 0x0C, 0x17, 0x0E, 0x4E, 0x37, 0xD2, 0x94,0x10, 0x09,
           0x2E, 0x22, 0x57, 0xFF, 0xC8, 0x0B, 0xB2, 0x70, 0x54])
P1 = " НаВашисходящийот1204".encode('utf-8')
P2 = "ВСеверныйфилиалБанкау".encode('utf-8')
c1 = xorbytes(P1, key)
c2 = xorbytes(P2, key)
print("c1 = ", c1)
print("c2 = ", c2)
P1_xor_P2 = xorbytes(c1,c2)
print("P1 ⊕ P2:", P1_xor_P2)
P1decrytion = decryption(c1, key)
P2decrytion = decryption(c2, key)
print("P1 decrypted= ", P1decrytion)
print("P2 decrypted= ", P2decrytion)
```

```
c1 =  b'%\xdc\x8a\xde\xfe\xe7@D\xa0\xd8\xa6\xf2\xef.I\xda7\xa0\xea\xd5\xb8\xc6\x81\x9f\xbe\x02,\xc0\xb0\xfe\x9c\x86}\xf99\x82D'
c2 =  b'\xd5\x9e\xc7\xaf\x9e\x82\x02&\xc0\xbc\xff\xa2\x87B\x19\x80b\xc9\x85\x81\xdc\xaf\xde\xf5\xe7jD\xa0\xd9\x95\xf2\xc6/x\xdb\x0f\xa0\xee\xd5\xbca'
P1 ⊕ P2: b'\xf0BMq`eBb`dYPhlPZUioTdi_jYhh`ikn@R\x81\xe2\x8d\xe4'
P1 decrypted=   НаВашисходящийот1204
P2 decrypted=  ВСеверныйфилиалБанкау
```

рис. 1 Код для шифрования и дешифрования сообщений

Функция xorbytes:

Выполняет операцию XOR для каждого байта текста и ключа. Если текст длиннее ключа, ключ повторяется.

Функция decryption:

Использует ту же операцию XOR для расшифровки сообщения с известным ключом.

Шифрование:

Для двух исходных сообщений P1 и P2, шифротексты c1 и c2 вычисляются через XOR с ключом.

Атака:

Вычисляется $P1 \oplus P2$, чтобы показать, как можно восстановить одно сообщение, если известно другое.

Вывод

В ходе выполнения работы я приобрела практические навыки использования режима одноразового гаммирования с применением одного ключа для кодирования двух сообщений.