МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра информационных технологий

ОТЧЕТ по лабораторной работе 8

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

по дисциплине «Информационная безопасность»

Выполнил:
Студент группы НПИбд-02-21
Студенческий билет № 1032205641
Сатлихана Петрити

Список содержания

Список изображений

Список изображений

Цель работы

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

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.

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

[7] def decrypt(ciphertext, key):
      return xor_bytes(ciphertext,key).decode('utf-8')

[8] key = bytes([0x05, 0x0C, 0x17, 0x7F, 0x0E, 0x4E, 0x37, 0xD2, 0x94, 0x10,
                 0x09, 0x2E, 0x22, 0x57, 0xFF, 0xC8, 0x0B, 0xB2, 0x70, 0x54])

[9] P1= " НаВашисходящийот1204".encode('utf-8')
    P2= " ВСеверныйфилиалБанка".encode('utf-8')

[10] C1= xor_bytes(P1,key)
     C2= xor_bytes(P2, key)

[11] print("C1:",C1)
     print("C2:",C2)

C1: b'%\xdc\x8a\xaf\xbe\x9e\xa5\x02$\xc1\x81\xfe\x9a\x86~\x19\x8eb\xce\x84\xb1\xdd\x98\xae\x87\x9e\x8f\x02-\xc0\xb7\xff\xa0f\xcd\xf8?'
C2: b'%\xdc\x85\xaf\xaf\x9e\x82\x02&\xc0\xbc\xff\xa2\x87B\x19\x80b\xc9\x85\x81\xdc\xaf\xaf\xb5\x9e\x8f\x02$\xc0\xb2\xfe\xb3\x87O\x18\xb6b\xca\x84\xb5'

P1_xor_P2 = xor_bytes(C1,C2)
print("P1 ⊕ P2:", P1_xor_P2)

P1 ⊕ P2: b"\x00\x00\x0f\x00\x11\x00'\x00\x02\x01=\x018\x01<\x00\x0e\x00\x07\x010\x017\x012\x00\x00\x00\t\x00\x05\x01\x13\xe1\x82\xe0\x89"

[13] P1_decrypted= decrypt(C1,key)
     P2_decrypted= decrypt(C2,key)

print("P1(DECRYPTED):",P1_decrypted)
print("P2(DECRYPTED):",P2_decrypted)

P1(DECRYPTED):  НаВашисходящийот1204
P2(DECRYPTED):  ВСеверныйфилиалБанка
```

рис. 1 Код для шифрования и дешифрования сообщений с использованием однократного гаммирования (XOR)

Функция xor_bytes:

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

Функция decrypt:

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⊕P2, чтобы показать, как можно восстановить одно сообщение, если известно другое.

Вывод

В результате выполнения работы я освоила на практике применение режима однократного гаммирования при использовании одного ключа для двух сообщений.