Лабораторная работа №8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

дисциплина: Информационная безопасность

Рыбалко Элина Павловна

Содержание

Список иллюстраций

Список таблиц

Цель работы

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

Объект/Предмет исследования

Криптография. Кодирование различных исходных текстов одним ключом.

Теоретическое введение

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте. [1] (#список-литературы).

Выполнение 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 (см. рис. -@fig:001).

```
[1] import string
    import random

    def f_hkey(text):
      return ' '.join(hex(ord(i))[2:] for i in text)

    def f_key(size):
      return ''.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))

    def encryption(text1, text2):
      txt1 = [ord(i) for i in text1]
      txt2 = [ord(i) for i in text2]
      return ''.join(chr(a^b) for a,b in zip (txt1, txt2))
```

```
[4] P1 = 'НаВашисходящийот1204'
    P2 = 'ВСеверныйфилиалБанка'

    #message = (input("Введите сообщение: "))

    key = f_key(len(P1))
    print("Используемый ключ: ", key)

    hex_key = f_hkey(key)
    print("Ключ в шестнадцатиричносм виде: ", hex_key)

    C1 = encryption(P1,key)
    C2 = encryption(P2,key)
    print("Шифротекст: ", C1)
    print("Шифротекст: ", C2)

    decrypt = encryption(C1, C2)
    D1 = encryption(decrypt,P1)
    D2 = encryption(decrypt,P2)
    print("Расшифрованное сообщение ", D1)
    print("Расшифрованное сообщение ", D2)
```

```
Используемый ключ:  rjoRQcRQyv97RfiqTq25
Ключ в шестнадцатиричносм виде:  72 6a 6f 52 51 63 52 51 79 76 39 37 52 66 69 71 54 71 32 35
Шифротекст:  ӟњӦБЙћГДчтѶѼѪџїгеС┐┌
Шифротекст:  ѠыњѠѥУӟКрвЁЌѪiђѠѥьJS
Расшифрованное сообщение  ВСеверныйфилиалБанка
Расшифрованное сообщение  НаВашисходящийот1204
```

Рис. 1: Разработанное приложение

Вывод

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

Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммир

2. Что будет при повторном использовании ключа при шифровании текста?

Повторное использование может привести ко взлому шифра.

3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним к

4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Злоумышленник получает возможность определить те символы сообщения P2, которые на
Несмотря на все преимущества криптографии с открытым ключом и вероятностного шифр

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

При использовании же криптосистем с открытым ключом стороны не обязаны встречатьс

Список литературы

1. Лабораторная работа №8
2. Использование однократного гаммирования
3. Руководство по формуле Cmd Markdown
4. Руководство по оформлению Markdown файлов