Отчёт по лабораторной работе 8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Гурбангельдиев Мухаммет НФИбд-03-18

Содержание

1 Цель работы **5**

2 Теоретические сведения **6**

3 Выполнение лабораторной работы **7**

4 Контрольные вопросы **8**

5 Выводы **9**

6 Список литературы **10**

List of Tables

List of Figures

3.1 Блок функции для расчетов 7
3.2 Блок данных и вывод результата 7

1 Цель работы

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

2 Теоретические сведения

Простейшей и в то же время наиболее надёжной из всех схем шифрования является так называемая схема однократного использования (см. рисунок 1), изобретение, которое чаще всего связывают с именем Г.С. Вернама [1].

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. С точки зрения теории криптоанализа, метод шифрования случайной однократной равновероятной гаммой той же длины, что и открытый текст, является невскрываемым (далее для краткости будем употреблять термин “однократное гаммирование”, держа в уме всё сказанное выше). Кроме того, даже раскрыв часть сообщения, дешифровщик не сможет хоть сколько-нибудь поправить положение – информация о вскрытом участке гаммы не даёт информации об остальных её частях [1].

Допустим, в тайной деловой переписке используется метод однократного наложения гаммы на открытый текст. “Наложение” гаммы – не что иное, как выполнение операции сложения по модулю 2 (xor) её элементов с элементами открытого текста. Эта операция в языке программирования C++ обозначается знаком , а в математике – знаком [1].

Гаммирование является симметричным алгоритмом. Поскольку двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, шифрование и дешифрование выполняется одной и той же программой [1].

3 Выполнение лабораторной работы

1. Написал блок функции для расчетов. (рис. 3.1)

```
In [20]: import string
         import random

In [21]: def hexx(text):
             return ' '.join(hex(ord(i))[2:] for i in text)
         def gen_key(size):
             return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(size))

         def encrypted(firstText,secondText):
             first_text=[ord(i) for i in firstText]
             second_text=[ord(i) for i in secondText]
             return ''.join(chr (a^b) for a,b in zip(first_text,second_text))
```

Figure 3.1: Блок функции для расчетов

2. Написал блок обработки данных. (рис. 3.2)

```
In [22]: P1 = "НаВашисходящийот1204"
         P2 = "ВСеверныйфилиалБанка"

         key=gen_key(len(P1))
         print(key)
         hex_key=hexx(key)
         print("Ключ в шестнадцатиричном виде: ",hex_key)

         C1= encrypted(P1,key)
         C2= encrypted(P2,key)

         print("Шифрованный текст: ",C1)
         print("Шифрованный текст: ",C2)

         decrypt=encrypted(C1,C2)
         print("Расфрованный текст: ",encrypted(decrypt,P2) )
         print("Расфрованный текст: ",encrypted(decrypt,P1) )

         DRMYSqBmFZbxB4KY2mdp
         Ключ в шестнадцатиричном виде:  44 52 4d 59 53 71 42 6d 46 5a 62 78 42 34 4b 59 32 6d 64 70
         Шифрованный текст:  љБцњЛщЃШ0ҙ3Э6ОЙvЛ_TD
         Шифрованный текст:  iѳ0ӽѦбѿЦѿОњуОЄѰшЂѐўp
         Расфрованный текст:  НаВашисходящийот1204
         Расфрованный текст:  ВСеверныйфилиалБанка
```

Figure 3.2: Блок данных и вывод результата

4 Контрольные вопросы

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

Сложить по модулю 2 оба шифротекста и декодировать первый текст используя полученное значение и известный второй текст.

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

Оба текста, шифрованные одним ключом будут подвержены риску взлома.

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

Шифруем оба текста одним ключом.

4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Подверженость риску взлома.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Используется меньше ключей.

5 Выводы

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

6 Список литературы

1. Гаммирование. Моделирование работы скремблера// URL: https://ami.nstu.ru/~gultyaeva/pszi/Materials/lab1.pdf (дата обращения: 10.12.2021).