Лабораторная работа №8

Дисциплина: Основы информационной безопасности

Коновалова Татьяна Борисовна

Содержание

1 Цель работы **5**

2 Теоретические данные **6**

3 Задание **7**

4 Выполнение лабораторной работы **8**

5 Выводы **11**

6 Библиография **12**

Список иллюстраций

4.1 Функция шифрования 8
4.2 Исходные данные 8
4.3 Случайный символьный ключ 9
4.4 Шифрование данных 9
4.5 Получение данных без ключа 9
4.6 Получение данных без ключа 10
4.7 Получение части данных 10

Список таблиц

1 Цель работы

Цель лабораторной работы — Освоить на практике применение однократного гаммирования при работе с различными текстами на одном ключе.

2 Теоретические данные

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. Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ⊠) между элементами гаммы и элементами подлежащего сокрытию текста.

3 Задание

1.Не зная ключа и не стремясь его определить, прочитать оба исходных текста; 2.Разработать приложение, позволяющее шифровать и дешифровать тексты в режиме однократного гаммирования; 3.Определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

4 Выполнение лабораторной работы

Лабораторную работу выполнила на языке Pythin 3 в среде Jupiter Notebook.

1.Создала функцию, которая осуществляет однократное гаммирование посредством побитового XOR (рис. [4.1]).

Ввод [22]:
```
def cript(text, key):
    if len(text) != len(key):
        return "Предупреждение: длины текста и ключа должны быть одинаковы!"
    result = ''
    for i in range(len(key)):
        p = ord(text[i]) ^ ord(key[i])
        result += chr(p)
    return result
```

Рис. 4.1: Функция шифрования

2.Задала две равные по длине текстовые строки и создала случайный символьный ключ такой же длины (рис. [4.2]) и (рис. [4.3]).

Ввод [23]:
```
text1 = "С Новым годом, друзья!"
text2 = "С Новым годом, семья!!"
```

Рис. 4.2: Исходные данные

```
Ввод [24]:
from random import randint, seed
seed(20)
key = ''
for i in range(len(text)):
    key += chr(randint(0, 100))
print(key)
```

```
▯(<J9!VQ)I▯▯44
```

Рис. 4.3: Случайный символьный ключ

3.Осуществила шифрование двух текстов по ключу с помощью написанной функции (рис. [4.4])

```
Ввод [25]:
cipher1 = cript(text1, key)
cipher2 = cript(text2, key)
print(cipher1, cipher2, sep="\n")
```

```
ѽwѹќСѪѪqпЗѽыn▯▯нэѓПΨS▯
ѽwѹќСѪѪqпЗѽыn▯▯шиЬЄѳk▯
```

Рис. 4.4: Шифрование данных

4.Создала переменную, которая, прогнав два шифрованных текста через побитовый XOR, поможет злоумышленнику получить один текст, зная другой, без ключа (рис. [4.5]) и (рис. [4.6]).

```
Ввод [26]:
vzlom = cript(cipher1, cipher2)
print(cript(vzlom, text1))
```

```
С Новым годом, семья!!
```

Рис. 4.5: Получение данных без ключа

```
Ввод [27]:  1  print(cript(vzlom, text2))

С Новым годом, друзья!
```

Рис. 4.6: Получение данных без ключа

5.Таким же способом я получила часть данных из исходных предложений (рис. [4.7])

```
Ввод [30]:  1  text2[2:13]

Out[30]: 'Новым годом'

Ввод [31]:  1  vzlom_part = cript(cipher1[2:13], cipher2[2:13])
            2  print(cript(vzlom_part, text2[2:13]))

Новым годом
```

Рис. 4.7: Получение части данных

5 Выводы

Освоила на практике применение однократного гаммирования при работе с различными текстами на одном ключе.

6 Библиография

СПИСОК ЛИТЕРАТУРЫ

1.Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: http://bugtraq.ru/library/books/attack1/index.html

2.Теоретические знания, приведённые в Лабораторной работе №8 - https://esystem.rudn.ru/pluginfile.php/2090135/mod_resource/content/2/008-lab_crypto-key.pdf

3.Запечников С. В. и др. Информационн~пасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006.

СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ

1.[Электронный ресурс] - доступ: https://codeby.school/blog/informacionnaya-bezopasnost/razgranichenie-dostupa-v-linux-znakomstvo-s-astra-linux

2.[Электронный ресурс] - доступ: https://debianinstall.ru/diskretsionnoe-razgranichenie-dostupa-linux/