Презентация по лабораторной работе №8

Коновалова Татьяна Борисовна

23 Октября 2023

РУДН, Москва, Россия

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

Цель лабораторной работы №8

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

Задачи лабораторной работы

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.

Ход лабораторной работы №8

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.

Функция шифрования

Создала функцию, которая осуществляет однократное гаммирование посредством побитового XOR

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. 1: Функция шифрования

Исходные данные

Задала две равные по длине текстовые строки и создала случайный символьный ключ такой же длины

Ввод [23]:

```
1 text1 = "С Новым годом, друзья!"
2 text2 = "С Новым годом, семья!!"
```

Рис. 2: Исходные данные

Исходные данные

Ввод [24]:

```
1 from random import randint, seed
2 seed(20)
3 key = ''
4 for i in range(len(text)):
5     key += chr(randint(0, 100))
6 print(key)
```

```
(<J9!VQ)I44
```

Рис. 3: Случайный символьный ключ

Шифрование данных

Осуществила шифрование двух текстов по ключу с помощью написанной функции

Ввод [25]:

```
1 cipher1 = cript(text1, key)
2 cipher2 = cript(text2, key)
3 print(cipher1, cipher2, sep="\n")
```

```
ѽwoyќCЖЖqnЗѽып□□нэґПΨS□
ѽwoyќCЖЖqnЗѽып□□шиЬЂѳk□
```

Рис. 4: Шифрование данных

Получение данных без ключа

Создала переменную, которая, прогнав два шифрованных текста через побитовый XOR, поможет злоумышленнику получить один текст, зная другой, без ключа

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

С Новым годом, семья!!
```

Рис. 5: Получение данных без ключа

Получение данных без ключа

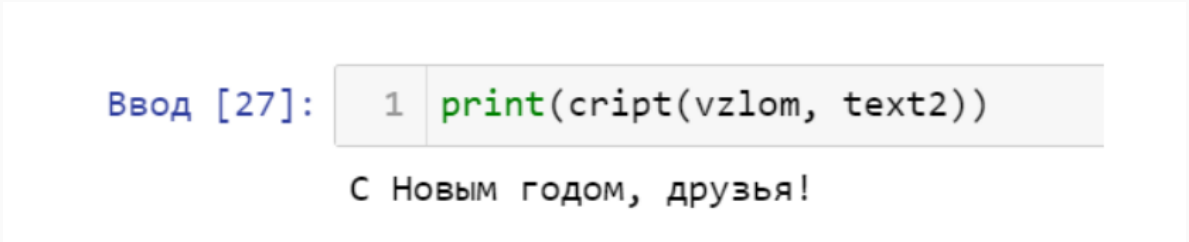

Рис. 6: Получение данных без ключа

Получение части данных

Таким же способом я получила часть данных из исходных предложений

```
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. 7: Получение части данных

Выводы

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

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/conte lab_crypto-key.pdf

СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ

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

Спасибо за внимание!