

Отчёт по лабораторной работе № 7

Дисциплина: Основы информационной безопасности

Перелыгин Сергей Викторович

Содержание

| | | |
|---|--------------------------------|----|
| 1 | Цель работы | 4 |
| 2 | Задание | 5 |
| 3 | Теоретическое введение | 6 |
| 4 | Выполнение лабораторной работы | 7 |
| 5 | Выводы | 9 |
| 6 | Библиография | 10 |

Список иллюстраций

| | | |
|-----|---|---|
| 4.1 | Приложение, реализующее режим однократного гаммирования | 7 |
| 4.2 | Вывод программы | 8 |

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Задание

- Сделать отчёт по лабораторной работе в формате Markdown.
- В качестве отчёта предоставить отчёты в 3 форматах: pdf, docx и md.

3 Теоретическое введение

Гаммирование - наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Основная формула, необходимая для реализации однократного гаммирования:

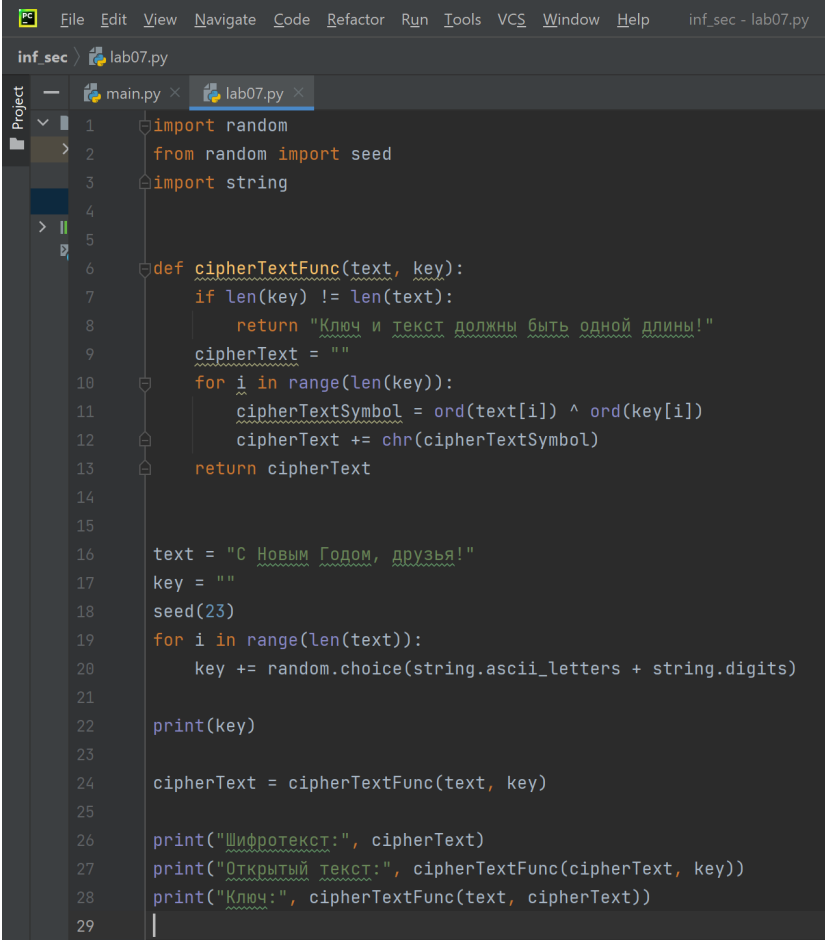
$C_i = P_i \text{ XOR } K_i$, где C_i - i -й символ зашифрованного текста, P_i - i -й символ открытого текста, K_i - i -й символ ключа.

Аналогичным образом можно найти ключ: $K_i = C_i \text{ XOR } P_i$. Необходимые и достаточные условия абсолютной стойкости шифра:

- длина открытого текста равна длине ключа
- ключ должен использоваться однократно
- ключ должен быть полностью случаен

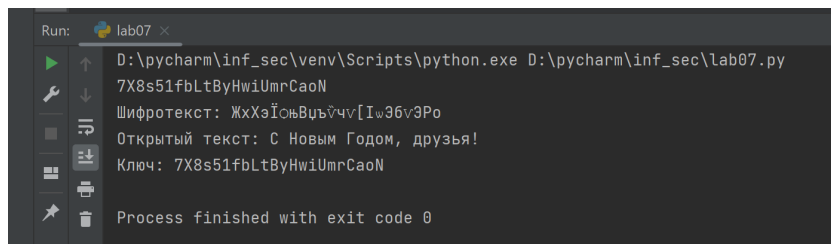
4 Выполнение лабораторной работы

1. Код программы (рис. 4.1) и вывод (рис. 4.2).



```
inf_sec > lab07.py
main.py x lab07.py x
1 import random
2 from random import seed
3 import string
4
5
6 def cipherTextFunc(text, key):
7     if len(key) != len(text):
8         return "Ключ и текст должны быть одной длины!"
9     cipherText = ""
10    for i in range(len(key)):
11        cipherTextSymbol = ord(text[i]) ^ ord(key[i])
12        cipherText += chr(cipherTextSymbol)
13    return cipherText
14
15
16 text = "С Новым Годом, друзья!"
17 key = ""
18 seed(23)
19 for i in range(len(text)):
20     key += random.choice(string.ascii_letters + string.digits)
21
22 print(key)
23
24 cipherText = cipherTextFunc(text, key)
25
26 print("Шифротекст:", cipherText)
27 print("Открытый текст:", cipherTextFunc(cipherText, key))
28 print("Ключ:", cipherTextFunc(text, cipherText))
29
```

Рис. 4.1: Приложение, реализующее режим однократного гаммирования



```
Run: lab07 x
D:\pycharm\inf_sec\venv\Scripts\python.exe D:\pycharm\inf_sec\lab07.py
7X8s51fbLtByHwiUmrCaoN
Шифротекст: ЖхХэЇсњВцъЇчv[Iw36v9Po
Открытый текст: С Новым Годом, друзья!
Ключ: 7X8s51fbLtByHwiUmrCaoN
Process finished with exit code 0
```

Рис. 4.2: Вывод программы

2. Пояснения к программе:

- Lines 1-3: импорт необходимых библиотек
- Lines 6-13: функция, реализующая сложение по модулю два двух строк
- Line 16: открытый/исходный текст
- Lines 17-22: создание ключа той же длины, что и открытый текст
- Lines 24-26: получение шифротекста с помощью функции, созданной ранее, при условии, что известны открытый текст и ключ
 - Line 27: получение открытого текста с помощью функции, созданной ранее, при условии, что известны шифротекст и ключ
 - Line 28: получение ключа с помощью функции, созданной ранее, при условии, что известны открытый текст и шифротекст

5 Выводы

Вывод: В ходе выполнения данной лабораторной работы я освоил на практике применение режима однократного гаммирования.

6 Библиография

- 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>
- Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. — Издательство ДМК, 1999. — URL: <http://bugtraq.ru/library/books/attack/index.html>
- Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячая линия -Телеком, 2006.
- Введение в информационную безопасность. Типы уязвимостей. (Д.Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Вводная лекция. Сетевая безопасность. Стек протоколов TCP/IP. (Д. Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Сетевая безопасность. Межсетевые экраны. (В. Иванов, МГУ)
- Практические аспекты сетевой безопасности. Сетевая безопасность. Системы обнаружения и фильтрации компьютерных атак (IDS/IPS). (Д. Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Контроль нормального поведения приложений. Security Enhanced Linux (SELinux) (В. Сахаров, МГУ)