Лабораторная работа №8

Царитова Нина, НПМбд-01-19

Содержание

Цель работы

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

Выполнение лабораторной работы

Создаём функцию, которая осуществляет однократное гаммирование посредством побитового XOR

```
def c(text, key):
  if len(text) != len(key):
    return "Ошибка"
  result = ''
  for i in range(len(key)):
    a = ord(text[i]) ^ ord(key[i])
    result += chr(a)
  return result
```

Задаём две равные по длине текстовые строки и создаём случайный символьный ключ такой же длины и осуществляем шифрование двух текстов по ключу с помощью написанной функции. Создаём переменную, которая, прогнав два шифрованных текста через побитовый XOR, поможет злоумышленнику получить один текст, зная другой, без ключа.

```
text1 = "С Новым годом, друзья!"
text2 = "Лабораторная работа№8!"

from random import randint, seed
seed(21)
key = ''
for i in range(len(text1)):
  key += chr(randint(0,5000))
print(key)
```

[illegible]

```
a1 = c(text1,key)
a2 = c(text2,key)
print(a1)
print(a2)
```

[illegible]

```
rez = c(a1,a2)
print(c(rez,text1))
```

```
Лабораторная работа№8!
```

```
print(c(rez,text2))
```

```
С Новым годом, друзья!
```

Выводы

Я освоила на практике применение режима однократного гаммирования при работе с несколькими текстами.

Список литературы

- 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. Информационн~пасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006.