Лабораторная работа №7

Царитова Нина

Содержание

Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

Лабораторная работа выполнена на языке Pythin 3 в среде Google Colab. 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 текстовую строку и создаём случайный символьный ключ такой же длины и запускаем функцию. В первом случае получаем зашифрованный текст. Далее, используя тот же самый ключ, осущвляем дешифровку текста. Так же, зная оригинальный текст и его шифорку, можем получить ключ.

Все действия осуществляются через одну и ту же функцию.

```
text = "С Новым годом, друзья!"

from random import randint, seed
seed(42)
key = ''
for i in range(len(text)):
  key += chr(randint(0,5000))
print(key)
```

```
[illegible]
```

```
a = c(text,key)
print(a)
```

```
[illegible]
```

```
print(c(a,key))
```

```
С Новым годом, друзья!
```

```
print(c(text,a))
```

```
[illegible]
```

Выводы

Я освоила на практике применение режима однократного гаммирования.

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.