

Презентация по лабораторной работе №8

Основы информационной безопасности

Закиров Н.Д.

29 мая 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Закиров Нурислам Дамирович
- Студент группы НКАбд-01-23
- Российский университет дружбы народов

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P_1 и P_2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C_1 и C_2 обоих текстов P_1 и P_2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Я выполнял лабораторную работу на языке программирования Python, используя функции, реализованные в лабораторной работе №7.

Выполнение лабораторной работы

Используя функцию для генерации ключа, генерирую ключ, затем шифрую два разных текста одним и тем же ключом

```
1 import random
2 import string
3
4 def generate_key_hex(text):
5     key = ''
6     for i in range(len(text)):
7         key += random.choice(string.ascii_letters + string.digits) #генерация цифры для каждого символа в тексте
8     return key
9
10 #для шифрования и дешифрования
11 def en_de_crypt(text, key):
12     new_text = ''
13     for i in range(len(text)): #проход по каждому символу в тексте
14         new_text += chr(ord(text[i]) ^ ord(key[i % len(key)]))
15     return new_text
16
17 t1 = 'С Новым Годом, друзья!'
18 key = generate_key_hex(t1)
19 en_t1 = en_de_crypt(t1, key)
20 de_t1 = en_de_crypt(en_t1, key)
21
22 t2 = "У Слона домов, орого!!"
23 en_t2 = en_de_crypt(t2, key)
24 de_t2 = en_de_crypt(en_t2, key)
```

Рис. 1: Шифрование двух текстов

В ходе лабораторной работы были освоены на практике навыки применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

...