Презентацияполабораторнойработе№1

Основыинформационнойбезопасности

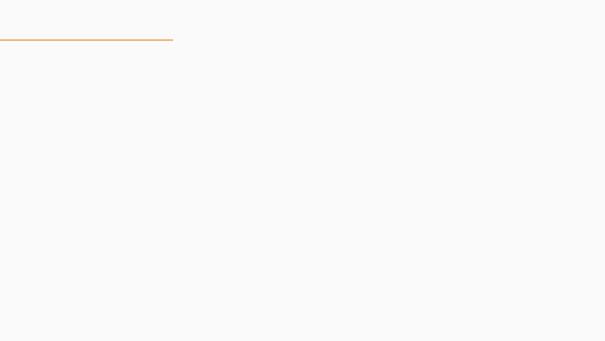
16 сентября 2025

Назармамадов У.ДЖ

Российский университет дружбы народов, Москва, Россия

1/7

Информация



- Назармамадов Умед Джамшедович
- студент группы НКАбд-03-23
- 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 P P тексты P P тексты P P дежиме однократного гаммирования.

Приложение должно определить вид шифротекстов ${}^{C}_{1}$ и ${}^{C}_{2}$ обоих текстов ${}^{P}_{1}$ и P2 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 выполняла лабораторную работу на языке программирования Python, используя функции, реализованные в лабораторной работе \mathbb{N}_2 7.

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

```
1 import random
 2 import string
 4 def generate key hex(text):
       key = "
       for i in range(len(text)):
           key += random.choice(string.ascii_letters + string.digits) #генерация цифры для каждого символа в тексте
       return key
10 #для шифрования и дешифрования
11 def en_de_crypt(text, key):
12
       new_text = "
       for i in range(len(text)): #npoxod no каждому симболу в тексте
14
           new_text += chr(ord(text[i]) ^ ord(key[i % len(key)]))
15
       return new_text
16
17 t1 = 'C 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, ororo!!"
```

Рис. 1: Шифрование двух текстов

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

:::