

Отчёт по лабораторной работе №7

Быстров Г. А.

21 октября 2023

Российский университет дружбы народов, Москва, Россия

- получить практические знания реализации режима однократного гаммирования;
- решить возникающие трудности и проблемы;
- практически получить полезный результат.

Разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования

1. Реализовал на языке Python программу (рис. 1).

```
import random
from random import seed
import string

def func(text, key):
    if len(key) != len(text):
        return "Разная длина"
    ctext = ''
    for i in range(len(key)):
        ctext_s = ord(text[i]) ^ ord(key[i])
        ctext += chr(ctext_s)
    return ctext

text = "С Новым Годом, друзья!"

key = ''
seed(23)
for i in range(len(text)):
    key += random.choice(string.ascii_letters + string.digits)

ctext = func(text, key)

print('Зашифрованный текст:', ctext)
print('Открытый текст:', func(ctext, key))
print('Известный ключ:', func(text, ctext))
```

Зашифрованный текст: ЖхХэЇОњВцъЎчV[IwЭ6VЭРо

Открытый текст: С Новым Годом, друзья!

Известный ключ: 7X8s51fbLtBvHwiUmrCaoN

- получил практические навыки для реализации режима однократного гаммирования.