Отчёт по лабораторной работе №8

Быстров Г. А.

21 октября 2023

Российский университет дружбы народов, Москва, Россия

Прагматика

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

Цель работы

Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования.

Задачи

1. Реализовал на языке Python программу (рис. 2).

```python
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

text1 = "С Новым Годом, друзья!"
text2 = "С днем рождения тебя!!"

key = ''
seed(23)
for i in range (len(text1)):
    key += random.choice(string.ascii_letters + string.digits)

ctext1 = func(text1, key)
ctext2 = func(text2, key)

print('Зашифрованный текст 1:', ctext1)
print('Зашифрованный текст 2:', ctext2)

print('Открытый текст 1:', func(ctext1, key))
print('Открытый текст 2:', func(ctext2, key))

ctextXOR = func(ctext1, ctext2)
print('Текст 1 XOR Текст 2:', ctextXOR)
```

Рис. 1: Код программы

Задачи

2. Реализовал на языке Python программу (рис. 2).

```
text1part1 = text1[3:6]
print('Часть открытого текста 1:', text1part1)

text2part1 = func(ctext1[3:6], ctext2[3:6])
print('Часть открытого текста 2:', func(text2part1, text1part1))
```

```
Зашифрованный текст 1: ЖхХэЇОъВцъЎчV[IwЭбVЭРо
Зашифрованный текст 2: ЖхЌюЁЙFTΘтЎьчяЦцЯчΘЮNo
Открытый текст 1: С Новым Годом, друзья!
Открытый текст 2: С днем рождения тебя!!
Текст 1 XOR Текст 2: )□□wЮ□□Дэ□Д□v□□З
Часть открытого текста 1: овы
Часть открытого текста 2: нем
```

Рис. 2: Код программы

Результаты

- получил практические навыки для реализации режима однократного гаммирования.