Лабораторная работа № 8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Артамонов Т. Е.

26 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Артамонов Тимофей Евгеньевич
- студент группы НКНбд-01-21
- Российский университет дружбы народов
- https://github.com/teartamonov

Цель работы

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

Теоретическое введение

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 P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 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.

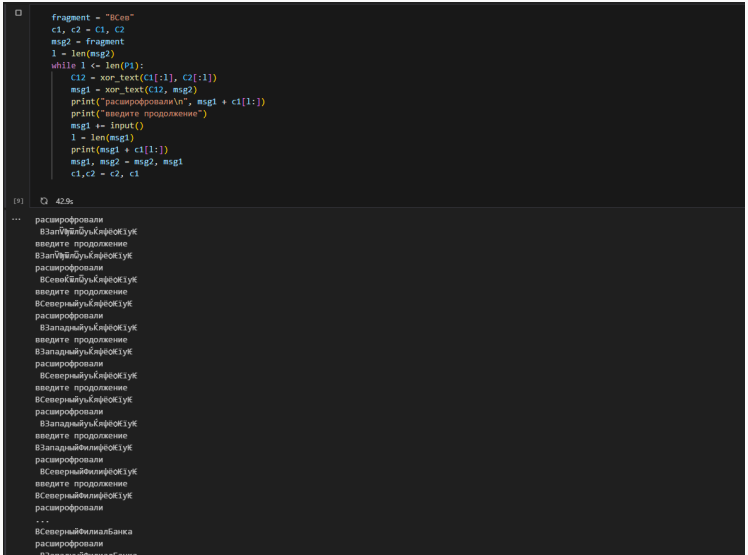
Выполнение лабораторной работы

Напишем функции на python и зададим переменные. (рис. (fig:001?))

```
import random
import string
✓ 0.0s

def xor_text(text, key):
    result = ""
    for i in range(len(text)):
        result += chr(ord(text[i]) ^ ord(key[i]))
    return result
✓ 0.0s

def key_gen(text):
    key = ""
    for i in range(len(text)):
        key += random.choice(string.ascii_letters + string.digits)
    return key
✓ 0.0s

def part_key(fragment, encrypted):
    first = xor_text(fragment, encrypted[:len(fragment)])
    return first + key_gen(encrypted[len(fragment):])
✓ 0.0s

text = "С новым годом, друзья!"
fragment = "С новым"

✓ 0.0s
```

Рис. 1: Код. Часть 1

Применим написанные функции для создания ключа, шифрования текста и дешифрования. (рис. (fig:002?))



Выводы

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