Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Артамонов Т. Е.

12 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.

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в “наложении” последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле. Например, в поле Галуа суммирование принимает вид операции “исключающее ИЛИ (XOR)”.

Выполнение лабораторной работы

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

```python
import random
import string
```
✓ 0.0s

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

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

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

```python
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?))

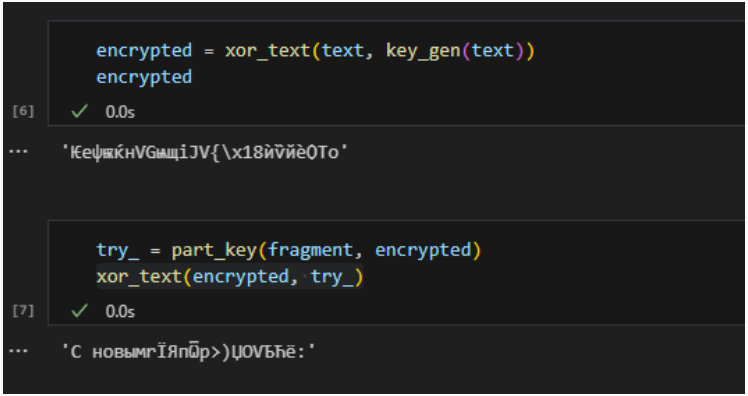

Рис. 2: Получили один из вариантов написания “С новым годом, друзья!”

Выводы

Освоили на практике применение режима однократного гаммирования.

Список литературы

1. Гаммирование [Электронный ресурс]. Wikimedia Foundation, Inc., 2024. URL: https://en.wikipedia.org/wiki/XOR_cipher.