Основы информационной безопасности. Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Демидова Е.А.

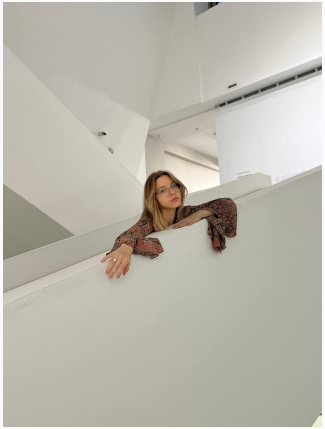
09.09.2023

Российский Университет дружбы народов

Информация

Докладчик

- Демидова Екатерина Алексеевна
- студентка группы НКНбд-01-21
- Российский университет дружбы народов
- https://github.com/eademidova



Вводная часть

Цели и задачи

Целью данной работы является освоить на практике применение режима однократного гаммирования.

Задание:

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Инструмент: Python

Выполнение лабораторной работы

Функции для реализации однократного гаммирования

```
def key_gen(text):
    alph = [chr(i) for i in range(1040,1104)] + [chr(i) for i in range(33,64)]
    key = "".join([random.choice(alph) for i in range(len(text))])
    return key

def encryption(text, key):
    return "".join([chr(ord(key[i])^ord(text[i])) for i in range(len(key))])

def part_key_gen(fragment, encrypted_text):
    key_start = encryption(fragment, encrypted_text[:len(fragment)])
    return key_start+key_gen(encrypted_text[len(fragment):])
```

Шифрование и дешифрование методом однократного гаммирования

```
text = "С новым годом, друзья!" # сообщение
key = key_gen(s) # ключ
encrypted_text = encryption(s, key) # зашифрованный текст
print(encrypted_text)

fragment = "С новым" # известный фрагмент сообщения
part_key = part_key_gen(fragment, encrypted_text) # ключ на основе фрагмента
guess = encryption(encrypted_text, part_key) # предположительный текст
print(guess)
```

Результаты

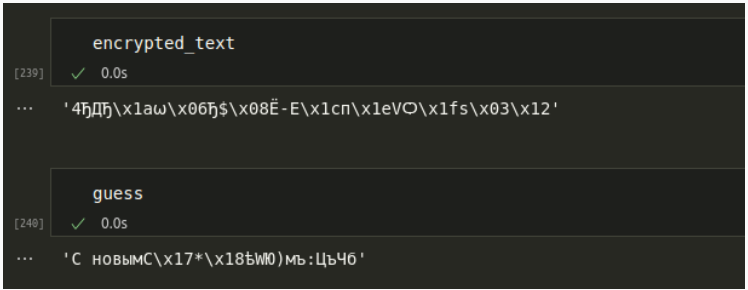


Рис. 1: Результаты работы программы

Заключение

Выводы

В результате выполнения работы были освоены практические навыки применения режима однократного гаммирования.

Список литературы

1. Ященко В. В. Введение в криптографию. МЦНМО, 2017. 349 с.