Лабораторная работа №7

Основы информационной безопасности

Иванов Сергей Владимирович, НПИбд-01-23

8 мая 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Освоить на практике применение режима однократного гаммирования.

Задание

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.

Выполнение работы

Функция генерации ключа

Для начала напишем функцию для генерации случайного ключа (рис. 1)

```python
import random
import string

# генерация ключа
1 usage
def generate_key(text):
    key = ''
    for i in range(len(text)):
        key += random.choice(string.ascii_letters + string.digits)
    return key
```

Рис. 1: Функция генерации ключа

Функция шифрования и дешифрования

Пишу функцию для шифровнаия и дешифрования текста. (рис. 2).

```
11  # шифрование и дешифрование текста
    3 usages
12  def en_de_crypt(text, key):
13      new_text = ''
14      for i in range(len(text)):
15          new_text += chr(ord(text[i]) ^ ord(key[i % len(key)]))
16      return new_text
```

Рис. 2: Функция шифрования и дешифрования

Поиск возможных ключей

Пишу функцию для поиска возможных ключей для фрагмента текста (рис. 3).

```
18  # функция для нахождения вохможных ключей
    1 usage
19  def find_keys(text, fragment):
20      possible_keys = []
21      for i in range(len(text) - len(fragment) + 1):
22          possible_key = ''
23          for j in range(len(fragment)):
24              possible_key += chr(ord(text[i + j]) ^ ord(fragment[j]))
25          possible_keys.append(possible_key)
26      return possible_keys
```

Рис. 3: Поиск возможных ключей

Проверка работы программы

Проверяем всех функций. Убеждаемся, все работает корректно. (рис. 4).

Рис. 4: Проверка работы программы

Вывод

Вывод

В ходе выполнения лабораторной работы мной было освоено на практике применение режима однократного гаммирования.