Лабораторная работа № 5.

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов.

Машков И. Е.

08 марта 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Машков Илья Евгеньевич
- Студент 2-го курс, группа НКАбд-03-23
- Российский университет дружбы народов
- 1132231984@pfur.ru
- https://github.com/7S7eVe7N7

Цель работы

Освоить на практике применение режима однократного гаммирования

Выполнение лабораторной работы

```python
import random
import string

def generate_key_hex(text):
    key = ''
    for i in range(len(text)):
        key += random.choice(string.ascii_letters + string.digits) #генерация цифры для каждого символа в тексте
    return key
```

Рис. 1: Функция генерации ключа

```python
#для шифрования и дешифрования
def en_de_crypt(text, key):
    new_text = ''
    for i in range(len(text)): #проход по каждому символу в тексте
        new_text += chr(ord(text[i]) ^ ord(key[i % len(key)]))
    return new_text
```

Рис. 2: Функция для шифрования текста

```python
def find_possible_key(text, fragment):
    possible_keys = []
    for i in range(len(text) - len(fragment) + 1):
        possible_key = ""
        for j in range(len(fragment)):
            possible_key += chr(ord(text[i + j]) ^ ord(fragment[j]))
        possible_keys.append(possible_key)
    return possible_keys
```

Рис. 3: Подбор возможных ключей для фрагмента

Выполнение лабораторной работы

```
t = 'С Новым Годом, друзья!'
key = generate_key_hex(t)
en_t = en_de_crypt(t, key)
de_t = en_de_crypt(en_t, key)
keys_t_f = find_possible_key(en_t, 'С Новым')
fragment = "С Новым"
print('Открытый текст: ', t, "\nКлюч: ", key, '\nШифротекст: ', en_t, '\nИсходный текст: ', de_t,)

print('Возможные ключи: ', keys_t_f)
print('Расшифрованный фрагмент: ', en_de_crypt(en_t, keys_t_f[0]))
```

```
Открытый текст:  С Новым Годом, друзья!
Ключ:  zAfqKSgvKyORVPr67bX2rX
Шифротекст:  ħaѻяφИħVjчѻЖ|RЂṽCʓѼнy
Исходный текст:  С Новым Годом, друзья!
Возможные ключи:  ['zAfqKSg', 'pħRG*\x10Ж', 'Zʓd&iHd', 'nљ\x05eЄ\x13{', 'XиFѬj\x0cG', '9ѻыfu0P', "zvEyI'V", 'ṽ0γZE^!p', 'yʌfRXзʓ', 'fħqTюЙ>', 'ZьwтѠIK',
'MъwЖ0<\x1d', 'K\\я<EjS', 'йr\x1fI\x13$B', 'өTj\x1f]5\x01', '#ї<QLvx']
Расшифрованный фрагмент:  С Новым,ЙСЊЧй(уБѐФЭњ
```

Рис. 4: Результат работы программы

Выводы

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