Отчёт по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Ханина Людмила Константиновна

Содержание

Цель работы

Освоить на практике применение режима однократного гаммирования

Выполнение лабораторной работы

1. Код, позволяющий шифровать и дешифровать данные в режиме однократного гаммирования:

```
import random
import string

def generateKey(text):
    key = ''
    for i in range(len(text)):
        key += random.choice(string.ascii_letters + string.digits)
    return key


def decryption(text, key):
    new_text = ''
    for i in range(len(text)):
        new_text += chr(ord(text[i]) ^ ord(key[i % len(key)]))
    return new_text

def findPossibleKey(text, fragment):
    possibleKeys = []
    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]))
        possibleKeys.append(possible_key)
    return possibleKeys

t = 'С Новым Годом, друзья!'
key = generateKey(t)
en_t = decryption(t, key)
de_t = decryption(en_t, key)
keys_t_f = findPossibleKey(en_t, 'С Новым')
fragment = "С Новым"
print('Открытый текст: ', t, "\nКлюч: ", key, '\nШифротекст: ', en_t, '\nИсходный текст: ', de_t, '\n')

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

Выводы

В ходе выполнения данной лабораторной работы я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux и проверила работу SELinux на практике совместно с веб-сервером Apache.