|  |
| --- |
| **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. |