Отчет по лабораторной работе №2. Шифры перестановки

Ильин Никита Евгеньевич

работы

Цель выполнения лабораторной

Цель выполнения лабораторной работы

Цель данной работы – научиться программировать шифры перестановки

Результат выполнения лабораторной работы

1. Для начала реализуется алгоритм маршрутного шифрования на языке Python (рис. (fig:001?)).

```
def encrypt(message, n):
   str list = [[]for in range(n)]
   cur str = 0
   for char in message:
       str_list[cur_str].append(char)
       cur_str += dir
       if cur str == 0 or cur str == n - 1:
           dir *= -1
   return ''.join([''.join(str) for str in str list])
def decrypt(message, n):
   str_list = [[]for _ in range(n)]
   cur_str = 0
   for char in message:
       str_list[cur_str].append(None)
       cur str += dir
       if cur_str == 0 or cur_str == n - 1:
           dir *= -1
    index = 0
   for str in str list:
       for i in range(len(str)):
           str[i] = message[index]
           index += 1
    decrypted_message = ''
   cur str = 0
   dir = 1
    for in range(len(message)):
```

Результат выполнения лабораторной работы

3. Затем реализуется алгоритм шифрования с помощью решеток на языке Python (рис. (fig:003?)).

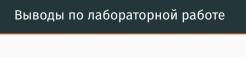
```
import numpy as np
rus='абвгдеёжзиклмнопрстуфхцчшшыыьэюя'
def encrypt(text, key, k):
    k_2=[x+1 \text{ for } x \text{ in } range(k**2)]
   matrix=[[0 for x in range(2*k)]for y in range(2*k)]
    matrix=np.array(matrix)
    for x in range(k**2):
        c=0
        for x in range(k):
            for y in range(k):
                matrix[x][v]=k 2[c]
                c+=1
        matrix=np.rot90(matrix)
    ds={k: 0 for k in k 2}
    dss={1:2,2:4,3:3,4:3}
    for x in range(k**2):
        for v in range(k**2):
            ds[matrix[x][y]]+=1
            if ds[matrix[x][y]]!=dss[matrix[x][y]]:
                matrix[x][v]=-1
                matrix[x][y]=0
    ct=0
    t=iter(text)
   matrixt=[['0' for v in range(k**2)] for x in range(k**2)]
    for d in range(4):
        for x in range(k**2):
            for v in range(k**2):
                if matrix[x][y]==0:
                     matrixt[x][y]=text[ct]
                    ct+=1
        matrix=np.rot90(matrix.-1)
    ps=[rus.index(x) for x in key]
```

Результат выполнения лабораторной работы

5. Затем реализуется алгоритм таблицы Виженера на языке Python (рис. (fig:005?)).

```
def genkey(text, key):
    key.replace(' ','')
    text.replace(' ','')
    key=list(key)
    if len(text) == len(key):
        return(key)
    else:
        for i in range(len(text)-len(key)):
            key.append(key[i%len(key)])
    return(''.join(key))
def encrypt(text,key):
    ct=[]
    text.replace(' ','')
    for i in range(len(text)):
        x=(ord(text[i])+ord(key[i]))%26
        x+=ord('A')
        ct.append(chr(x))
    return(''.join(ct))
def decrypt(ct,key):
    ot=[]
    for i in range(len(ct)):
        x=(ord(ct[i])-ord(key[i])+26)%26
        x+=ord('A')
```

Выводы по лабораторной работе



Реализованы программные алгоритмы шифров перестановки.