Вторая лабораторная работа. Шифры перестановки

НПИмд-01-23

Бармина Ольга Константиновна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Цель данной работы - ознакомиться с шифрами перестановки, а также научиться применять их на практике.

2 Задание

1. Реализовать маршрутное шифрование
2. Реализовать шифрование с помощью решеток
3. Реализовать шифрование с использованием таблицы Вижинера

3 Теоретическое введение

Шифры перестановки преобразуют открытый текст в криптограмму путем перестановки его символов. Способ, каким при шифровании переставляются буквы открытого текста и является ключом шифра. Важным требования является равенство длин ключа исходного текста.

4 Выполнение лабораторной работы

1. Произведено ознакомление с шифрами перестановки по методическим материалам курса

2. Прописан код для маршрутного шифрования на языке программирования Python. Выводим на экран результат применения.

```
def marsh(text, n, m, pas):
    text = text.lower().replace(' ', '')
    alphabet = 'абвгдеёжзийклмнопрстуфхцчшщъыьэюя'
    if len(text) < n*m:
        text += alphabet[:m*n - len(text)]
    c = iter(text)
    matrix = [[next(c) for y in range(m)] for x in range(n)]
    mat_pas = [alphabet.index(x) for x in pas]
    mat_pas_sort = sorted(mat_pas)

    res = ''
    for c1 in mat_pas_sort:
        for i in range(n):
            res += matrix[i][mat_pas.index(c1)]
    return res
```

```
test_text = 'Нельзя недооценивать противника'
marsh(test_text, 5, 6, 'пароль')
```

```
'еенпнзоатаьовокннеьвлдирияцтиа'
```

Рис. 4.1: Маршрутное шифрование

4. Прописан код для шифрования с помощью решеток на языке программирования Python. Выводим на экран результат применения.

```python
import numpy as np

def resh(text, pas, k=2):
    text = text.lower().replace(' ', '')
    k_2 = [x+1 for x in range(k**2)]
    matr = [[0 for x in range (2*k)] for y in range(2*k)]
    matr = np.array(matr)

    for x in range(k**2):
        c = 0
        for x in range(k):
            for y in range(k):
                matr[x][y] = k_2[c]
                c += 1
        matr = np.rot90(matr)
    mv = {k: 0 for k in k_2}
    mv_2 = {1:2, 2:4, 3:3, 4:3}
    for x in range(k**2):
        for y in range(k**2):
            mv[matr[x][y]] += 1
            if mv[matr[x][y]] != mv_2[matr[x][y]]:
                matr[x][y] = -1
            else:
                matr[x][y] = 0
```

Рис. 4.2: Шифрование с помощью решеток

```python
    ct = 0
    t = iter(text)
    matr2 = [['0' for x in range (2*k)] for y in range(2*k)]
    for v in range(4):
        for x in range(k**2):
            for y in range(k**2):
                if matr[x][y] == 0:
                    matr2[x][y] = text[ct]
                    ct += 1
        matr = np.rot90(matr, -1)
    alphabet = 'абвгдеёжзийклмнопрстуфхцчшщъыьэюя'
    password = [alphabet.index(x) for x in pas]
    pas_sort = sorted(password)

    res = ''
    for c1 in pas_sort:
        for i in range(k**2):
            res += matr2[i][password.index(c1)]
    return res
```

```python
test_text = 'договор подписали'
resh(test_text, 'шифр', 2)
```

```
'овордлгпапиосдои'
```

Рис. 4.3: Результат применения 2

6. Прописан код для шифрования с использованием таблицы Вижинера на языке программирования Python. Выводим на экран результат применения.

```python
def gen_key(m, pas):
    m = m.lower().replace(' ', '')
    pas = pas.lower().replace(' ', '')
    pas = list(pas)
    if len(m) == len(pas):
        return pas
    else:
        for i in range(len(m)-len(pas)):
            pas.append(pas[i%len(pas)])
    pas = ''.join(pas)
    return pas
```

```python
def vigion(text, pas):
    v = []
    text = text.lower().replace(' ', '')
    for i in range(len(text)):
        x = (ord(text[i]) + ord(pas[i])) % 32 + ord('a')
        v.append(chr(x))
    v = ''.join(v)
    return v
```

```python
test_text = 'криптография серьезная наука'
key = 'математика'`
gen_key(test_text, key)
```

```
'математикаматематикаматема'
```

```python
vigion(test_text, gen_key(test_text, key))
```

```
'цръфюохшкффягкььчпчалнтшца'
```

Рис. 4.4: Таблица Вижинера

5 Выводы

В рамках данной лабораторной работы было произведено ознакомление с шифрами перестановки. Шифры были реализованы на языке программирования Python.

6 Список литературы

1. Методические материалы курса