Шифры перестановки

Цель лабораторной работы

Изучить шифры перестановки.

Задачи лабораторной работы

1. Реализовать шифр маршрутным способом.
2. Реализовать шифр с помощью решеток.
3. Реализовать шифр с помощью таблицы Виженера.

Ход лабораторной работы

Маршрутное шифрование

1. Реализуем шифр маршрутным способом. (рис. @fig:001)(рис. @fig:002).

```
import string

k = input().split()
k[0] = int(k[0])
k[1] = int(k[1])
password = list(k[2])
size = k[0]*k[1]
i = -k[0]
indexes = []
out = []

col = [ [0]*k[0]  for i in range(k[1]+1) ]

inp = list(input().replace(" ", ""))
for t in range(size - len(inp)):
  inp.append(inp[-1])

for t in range(len(inp) - size):
  inp.pop()

for n in range(k[1]):
  i += k[0]
  for m in range(k[0]):
    col[n][m] = inp[i + m]
```

```
for m in range(k[0]):
  col[k[1]][m] = password[m]

map = password.copy()
map.sort()
for t in map:
  for r in password:
    if t == r:
      indexes.append(password.index(r))
for q in indexes:
  for t in range(k[1]):
    out.append(col[t][q])

print(out)
```

```
6 5 пароль
нельзя недооценивать противника
['е', 'е', 'н', 'п', 'н', 'з', 'о', 'а', 'т', 'а', 'ь', 'о', 'в', 'о', 'к', 'н', 'н', 'е', 'ь', 'в', 'л', 'д', 'и', 'р', 'и', 'я', 'ц', 'т', 'и', 'а']
```

1. Реализуем шифр с помощью решеток. (рис. @fig:003)(рис. @fig:004).

```
import string
import numpy as np

k1 = int(input())
inp1 = list(input().replace(" ", ""))
password = input()
m = len(inp)

print(k1, inp1)

q = np.arange(k**2).reshape(k, k) + 1
cyph = np.vstack([np.hstack([q, np.rot90(q, k = 3)]), np.hstack([np.rot90(q), np.rot90(q, k = 2)])])
for i in range(k**2):
  index = np.random.randint(3)
  a1 = np.where(cyph == (i+1))[0][index]
  b1 = np.where(cyph == (i+1))[1][index]
  cyph[a1][b1] = 0

cyph1 = cyph
cyph2 = np.rot90(cyph, k = 3)
cyph3 = np.rot90(cyph, k = 2)
cyph4 = np.rot90(cyph)
index1 = np.where(cyph1 == 0)
index2 = np.where(cyph2 == 0)
index3 = np.where(cyph3 == 0)
index4 = np.where(cyph4 == 0)
o = np.hstack([index1, index2, index3, index4])
outcyph = np.empty([2*k, 2*k], dtype = "object")

print(cyph1)
```

```
for i in range(4):
  for j in range(k**2):
    outcyph[o[0][(k**2)*i + j]][o[1][(k**2)*i + j]] = inp[(k**2)*i + j]
print(outcyph)
map = sorted(list(password))
listofindex = []
for i in map:
  listofindex.append(password.find(i))
out = ''
for i in listofindex:
  for j in range(len(outcyph)):
    out += outcyph[j][i]

print(out)
```

```
2
договор подписали
шифр
2 ['д', 'о', 'г', 'о', 'в', 'о', 'р', 'п', 'о', 'д', 'п', 'и', 'с', 'а', 'л', 'и']
[[1 2 3 1]
 [3 4 0 2]
 [0 4 4 0]
 [0 3 2 1]]
[['в' 'о' 'с' 'о']
 ['д' 'а' 'д' 'п']
 ['о' 'и' 'р' 'г']
 ['о' 'п' 'л' 'и']]
оаипопгисдрлвдоо
```

1. Реализуем шифр с помощью таблицы Виженера. (рис. @fig:005).

```
import string
import numpy as np

alphabet = "абвгдежзийклмнопрстуфхцчшщьыэюя"
inp1 = input().replace(" ", "")
password = input()
p = len(password)

for i in range(len(inp1) - p):
  password += password[i]

out = []
for t in range(len(inp1)):
  r = alphabet[(alphabet.index(inp1[t]) + alphabet.index(password[t])) % len(alphabet)]
  out.append(r)

print(out)
```

```
криптография серьезная наука
математика
['ц', 'р', 'ь', 'ф', 'я', 'о', 'х', 'ш', 'к', 'ф', 'ф', 'я', 'д', 'к', 'э', 'ь', 'ч', 'п', 'ч', 'а', 'л', 'н', 'т', 'ш', 'ц', 'а']
```

Выводы

Были изучены шифры перестановки на примере маршрутного шифра, шифра с помощью решеток и шифрования с помощью таблицы Виженера.