Шифры перестановки

Гурбангельдиев Мухаммет [1]

2022 Moscow, Russia

[1]RUDN University, Moscow, Russian Federation

Цель работы

цель работы

Реализация маршрутного шифра, решетчатого шифра и таблицы Виженера.

Задачи

Задачи

1. Реализовать шифрование с помощью решеток.
2. Реализовать маршрутное шифрование.
3. Реализовать шифр Виженера.

Результат

Результат

```python
# Encryption
def encryptMessage(msg, key):
    cipher = ""


    msg = msg.replace(' ', '')

    # берём длину текста
    msg_len = int(len(msg))

    # создаём список букв этого текста
    msg_lst = list(msg)

    # сортируем буквы ключа по алфавиту
    key_lst = sorted(list(key))

    # считаем количество стобцов
    col = len(key)

    # считаем количество строк
    if msg_len % col == 0:
        row = int(msg_len / col)
    else:
        row = int(msg_len // col) + 1

    # добавляем английскую a, если наша таблица не полная.
    fill = int((row * col) - msg_len)
    msg_lst.extend('a' * fill)

    # создадим матрицу нужного размера для шифрования
    matrix = [msg_lst[i: i + col] for i in range(0, len(msg_lst), col)]

    # читаем получившуюся матрицу постолбцово (?)

    for i in range(col):
        # так как до этого мы сортировали в алфавитном порядке,
        # теперь нам надо найти эти буквы в исходном ключе
        # и взять их порядковый номер на рукаве
        curr_idx = key.index(key_lst[i])
        # и соединить это всё в одну строку
        cipher += ''.join([row[curr_idx] for row in matrix])

    return cipher
```

Результат

```
while True:
    msg = input(bold + "What message do you want to encrypt?\n" + end + "Note that only russian and english characters and space
    if (False in [x in a for x in msg]):
        continue
    else:
        break

while True:
    key = input(bold + "\nEnter the key\n" + end + "Note that repeated characters are prohibited:\n")
    if len(set(key)) != len(key):
        continue
    else:
        break

print("\nYour encrypted message is: " + bold + ul + encryptMessage(msg, key))
```

```
What message do you want to encrypt?
Note that only russian and english characters and space are allowed:
poka

Enter the key
Note that repeated characters are prohibited:
poka

Your encrypted message is: akop
```

Figure 2: Получение шифрования

Результат

Расшифровка

```
msg = input("What message do you want to decrypt? ")
key = input("\nEnter the key: ")

print("\nYour decrypted message is: " + bold + ul + decryptMessage(msg,key))
```

```
What message do you want to decrypt? poka

Enter the key: poka

Your decrypted message is: akop
```

Figure 3: Получение расшифровки

Результат

Ввод [36]:

```
while True:
    msg = input("What message do you want to decrypt? ")
    if (False in [x in a1 for x in msg]):
        continue
    else:
        msg = msg.upper()
        break

while True:
    key = input("\nEnter the key: ")
    if (False in [x in a1 for x in msg]):
        continue
    else:
        key = key.upper()
        break

keyg = genKey(msg,key)
print("\nYour decrypted message is: " + bold + ul + unvig(msg,keyg))
```

```
What message do you want to decrypt? ECUA

Enter the key: ECUA

Your decrypted message is: AAAA
```

Figure 4: Получение шифрования текста методом Виженера

Вывод

Реализовал шифрование с помощью решеток, маршрутное шифрование и шифр Виженера

Спасибо за внимание