

Отчёт по лабораторной работе 2

Хамбалеев Булат Галимович

1 октября, 2022

Реализовать программно алгоритмы маршрутного шифрования и шифра Виженера.

Задание подразумевает реализацию алгоритма шифров на языке программирования.

Выполнение лабораторной работы

Выполнение лабораторной работы

1. Реализуем класс `marshrut` маршрутного шифрования.(рис. 1)

```
class marshrut():  
    def __init__(self,password):  
        self.m = 0  
        self.n = len(password)  
        self.password = password  
        self.table = []  
  
    def code(self, text):  
        table = []  
        while text:  
            table.append(list(text[:self.n]))  
            text = text[self.n:]  
        while len(table[-1]) < self.n:  
            table[-1].append('a')  
        self.m = len(table)  
        self.table = table  
  
        d = {k:v for k,v in zip(self.password,range(self.n))}  
        a = sorted(d)  
        b = [d[i] for i in a]  
        ans = []  
  
        for j in b:  
            for i in range(self.m):  
                ans.append(self.table[i][j])  
        ans = ''.join(ans)  
  
        return ans,self.m,self.n  
  
    def decode(self,text,key,m,n):  
        d = {k:v for k,v in zip(key,range(n))}  
        a = sorted(d)  
        b = [d[i] for i in a]  
  
        table = [['_' for i in range(n)] for j in range(m)]  
        k=0
```

2. Проверим работу алгоритма. (рис. 2)

```
Ввод [168]: a = marshrut("пароль")
Ввод [169]: a.code("нельзя доносить противника")
Out[169]: ('еенпзоатаювокинъевдиряцтва', 5, 6)
Ввод [170]: a.decode('еенпзоатаювокинъевдиряцтва', "пароль", 5, 6)
Out[170]: 'нельзя доносить противника'

Ввод [ ]:
Ввод [171]: b = marshrut("булат")
Ввод [172]: b.code("пойдёте по границе улицы")
Out[172]: ('длауапимийераёеоеаотгнц', 5, 5)
Ввод [173]: b.status()
5 5 [['н', 'о', 'а', 'а', 'а'], ['н', 'т', 'е', 'н', 'о'], ['н', 'р', 'а', 'е'], ['н', 'н', 'а', 'у', 'л'], ['н', 'ц', 'е', 'а', 'а']]
Ввод [173]: b.decode('длауапимийераёеоеаотгнц', "булат", 5, 5)
Out[173]: 'пойдёте по границе улицы'
Ввод [170]: len("пойдёте по границе улицы")
Out[170]: 23
Ввод [177]: c = marshrut("куликов")
Ввод [178]: c.code("давайте добавим больше лабораторных курс")
Out[178]: ('ялоуамшаваддлеткабартыркаоолоуаюнс', 6, 7)
Ввод [180]: c.decode('ялоуамшаваддлеткабартыркаоолоуаюнс', "куликов", 6, 7)
Out[180]: 'давайте добавим больше лабораторных курсов'
```

Figure 2: рис.2. Маршрутное шифрование в действии.

3. Реализуем класс шифра Виженера. (рис. 3)

```
Ввод [317]: class Vigenere():  
  
    def __init__(self):  
        self.string = 'АБВГДЕЖЙЙКЛНОПРСТУХЦЧДШЬЪЭЮЯ'  
        string = 'АБВГДЕЖЙЙКЛНОПРСТУХЦЧДШЬЪЭЮЯ'  
        abc = []  
        for i in range(32):  
            abc.append(list(string))  
            string = string[1:] + string[0]  
  
        self.abc = abc  
  
    def code(self, text, password):  
        text = text.upper()  
        password = password.upper()  
        while ' ' in text:  
            text = text.replace(' ', '')  
        s = ''  
        if len(text) > len(password):  
            while len(text) > len(password):  
                password = password + password  
        while len(password) > len(text):  
            password = password[: -1]  
        i = [self.string.find(password[k]) for k in range(len(password))]  
        j = [self.string.find(text[k]) for k in range(len(text))]  
        return ''.join([self.abc[a][b] for a, b in zip(j, i)])  
  
    def decode(self, text, password):  
        password = password.upper()  
        if len(text) > len(password):  
            while len(text) > len(password):  
                password = password + password  
        while len(password) > len(text):  
            password = password[: -1]  
        i = [self.string.find(password[k].upper()) for k in range(len(password))]  
        j = [self.abc[k].index(p) for k, p in zip(i, text)]  
        return ''.join([self.string[l] for l in j])
```

Figure 3: рис.3. Класс Виженер.

4. Проверим работу алгоритма.(рис. 4)

```
Ввод [2]: i = Vigenere()

Ввод [3]: i.code("криптографиясерьезнаянаука","математика")
Out[3]: 'ЦРЪАХОХХХОАГКЪАЧПНЛНТЩА'

Ввод [4]: i.decode('ЦРЪАХОХХХОАГКЪАЧПНЛНТЩА','математика')
Out[4]: 'КРИПТОГРАФИЯСЕРЬЕЗНАУКА'

Ввод [5]: i.code("я с удовольствием провел время","булат")
Out[5]: 'АДДАГАБЪДГХУХХЕРГШЕЧЮБЕА'

Ввод [6]: i.decode('АДДАГАБЪДГХУХХЕРГШЕЧЮБЕА','булат')
Out[6]: 'ЯСУДОЛЬСТВИЕНПРОВЕЛВРЕЯ'

Ввод [7]: i.code('АЛМБЛХОРОШОПЛОХУАТЬ','кухнязаполнена')
Out[7]: 'ЙАУОКЕХЖОУЮОЖОНСБ'

Ввод [8]: i.decode('ЙАУОКЕХЖОУЮОЖОНСБ','кухнязаполнена')
Out[8]: 'АЛМБЛХОРОШОПЛОХУАТЬ'

Ввод [ ]:
```

Figure 4: рис.4. Шифр Виженера в действии.

Спасибо за внимание