

Шифр на графах

Проаспэт А.Г.

ДКО-102

Задача с одной из олимпиад по криптографии

Шифр на графе

Для зашифрования натурального числа m используется граф, представляющий собой множество вершин, некоторые из которых соединены друг с другом прямой линией. Вершины графа, соединенные друг с другом, называют *соседними*. Зашифрование состоит в выполнении следующих действий. В вершины графа записываются натуральные числа так, чтобы их сумма была равна m . Затем к числу в каждой вершине прибавляются числа в соседних вершинах. В результате получается граф, в котором «зашифровано» число m . Пример: для зашифрования числа 8 будем использовать граф на рис. 1. В его вершины поместим числа, сумма которых равна 8 (рис. 2). Затем к каждому числу прибавим числа в соседних вершинах. Результат зашифрования указан на рис. 3. На рис. 4 приведен результат зашифрования некоторого числа. Найдите его.

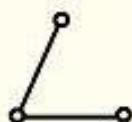


Рис. 1

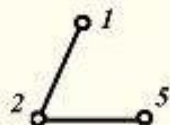


Рис. 2

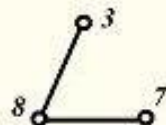


Рис. 3

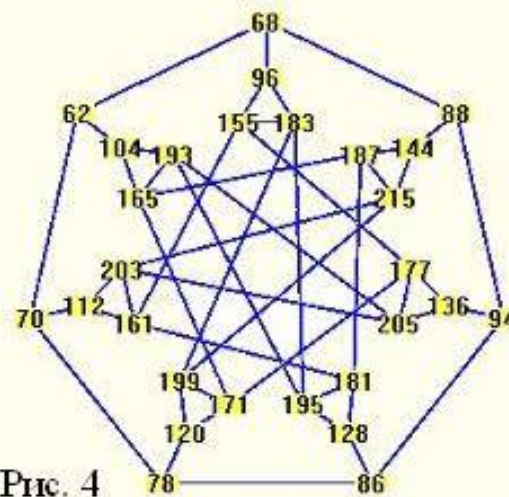


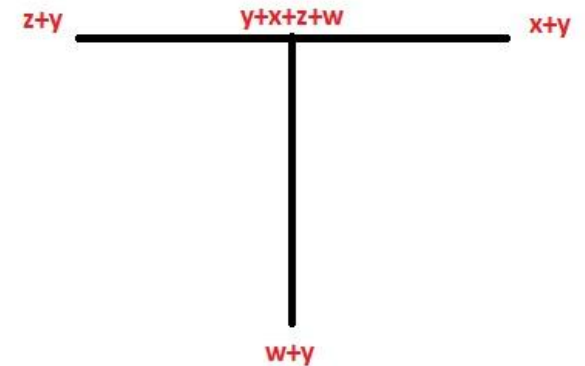
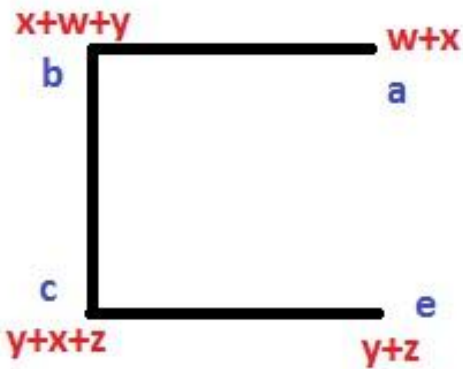
Рис. 4

Рассмотрим самые простые способы применения этого шифра

Если у графа три
вершины:



Если у графа четыре вершины



Выведем формулы

$$\begin{aligned} y &= b - a \\ x &= c - e \\ w &= a - x = a - c + e \\ z &= e - y = e - b + a \end{aligned}$$

$$\begin{aligned} x - y &= a - e \\ x - w &= c - e \\ x - z &= b - e \\ y - z &= b - a \\ w - y &= a - c \end{aligned}$$

$$\begin{aligned} z + w &= b - a \\ x + w &= b - c \\ z - w &= c - e \\ 2z &= b - a + c - e \\ 2w &= e - c - b + a \\ x &= b - c - w \\ y &= b - x - y - z \end{aligned}$$

Зачем нам шифровать числа?

А=1 Р=19

Б=2 С=20

В=3 Т=21

Г=4 У=22

Д=5 Ф=23

Е=6 Х=24

Ё=7 Ц=25

Ж=8 Ч=26

З=9 Щ=27

И=10 Ъ=28

Й=11 Ы=29

К=12 Ь=30

Л=13 Э=31

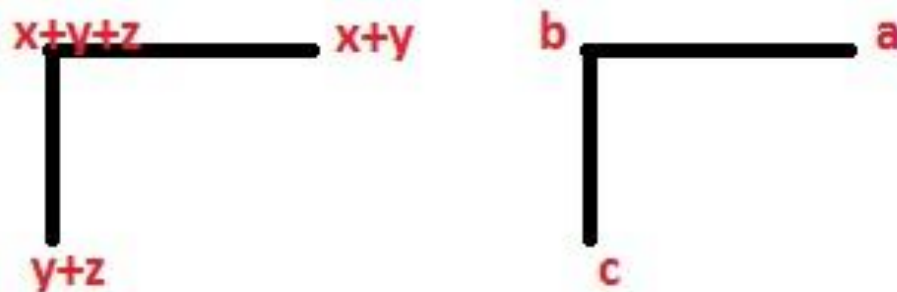
М=14 Ю=32

Н=15 Я=33

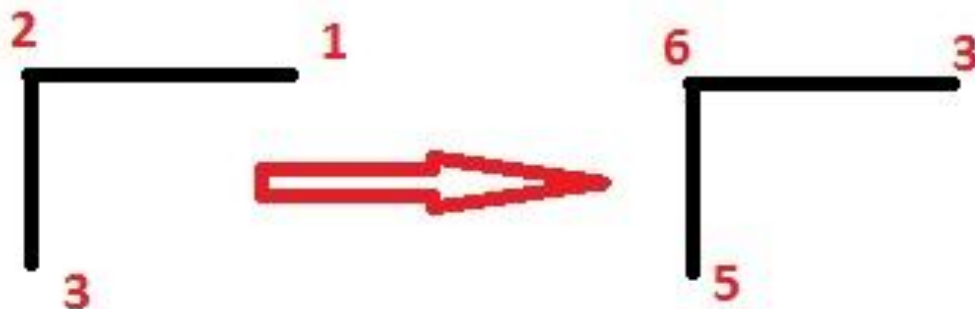
О=17 . =34

П=18 ? =35

_ =36



Пример: зашифруем 6



$$a=x+y ; b=x+y+z ; c=y+z$$

$$z=b-a$$

$$x=b-c$$

$$y=a-x=a-b+c$$

$$\text{проверим: } x+y-x-y-z+y-z=y$$

Алгоритм расшифровки

- Вводим с клавиатуры через запятую 6-значные числа (если составная часть однозначная, дополнять нулями)
- Разбиваем строку на 2-значные числа
- Каждое число разбиваем на 3 двузначных, используя операции деления на степени 10 с остатком
- Применяем формулы
- Складываем найденные числа, переводим цифры в символы
- Из символов складываем строку
- Выводим найденную строку

Алгоритм зашифровки

- Вводим с клавиатуры строку
- Каждый символ преобразовываем в число
- Зашифровываем числа в вершины графа
- Складываем числа в 6-значные, умножая на степени 10
- Выводим конечные 6-значные числа как строку

Пример:

МАТЕМАТИКА -> 131413010100022120030605131413010100022120081006101207010100

14, 1, 21, 6, 14, 21, 10, 12, 1

14=1+12+1 ШИФР: 13, 14, 13

1=1+0+0 ШИФР: 1, 1, 0

21=1+1+19 ШИФР: 2, 21, 20

6=1+2+3 ШИФР: 3, 6, 5

10=4+4+2 ШИФР: 8, 10, 6

12=5+5+2 ШИФР: 10, 12, 7

Вывод: 131413,010100,022120,030605, 131413,010100, 022120,081006,101207,010100

Расшифруем:

14-13=1 ; 14-13=1; 14-2=12

1+1+12=14 – это буква М

1-1=0 ; 1-0=1; 1-1=0

1+0+0=1 – это буква А

6-3=3 ; 6-5=1; 5-3=2

3+1+2=6 – это буква Е

***Благодарю за
внимание!***