In [1]:
```
p=23; g=7;
```

In [2]:
```
#Bob envía un mensaje a Alice
```

In [5]:
```
a=13;
```

In [6]:
```
A=g^a % p; A
```

Out[6]: 20

In [9]:
```
(p,g,A) #clave publica Alice
```

Out[9]: (23, 7, 20)

In [8]:
```
(a) #clave privada Alice
```

Out[8]: 13

In [11]:
```
b=9; M=5; #Bob quiere enviar un mensaje a Alice y escoge b
```

In [12]:
```
B=g^b % p; B
```

Out[12]: 15

In [13]:
```
C=(A^b)*M % p; C
```

Out[13]: 2

In [14]:
```
(B,C) #Bob envia este mensaje a Alice
```

Out[14]: (15, 2)

In [15]:
```
(B^(p-1-a))*C % p  #Alice recupera el mensaje M
```

Out[15]: 5

In [16]:
```
C*(B^a)^-1 % p #alternativamente podría hacer Alice para recuperar M
```

Out[16]: 5

In [ ]:
```

```