In [1]:
```
p = random_prime(2^33, 2^32)
p
```

Out[1]:
```
5191492591
```

In [2]:
```
q = random_prime(2^32, 2^31)
q
```

Out[2]:
```
340891391
```

In [3]:
```
n = p*q
```

In [4]:
```
m =(p-1)*(q-1) # euler_phi(n)
m
```

Out[4]:
```
1769735125179800100
```

In [5]:
```
e = randint(2,m)
while gcd(e, m) != 1:
    e = randint(2,m)
e, gcd(e, m)
```

Out[5]:
```
(405337480659039757, 1)
```

In [6]:
```
d = power_mod(e, -1, m)
d
```

Out[6]:
```
670234520228330293
```

In [7]:
```
mens = 1234
```

In [8]:
```
cif = power_mod(mens,e, n)
cif
```

Out[8]:
```
1447088323435171140
```

In [9]:
```
power_mod(cif, d, n)
```

Out[9]:
```
1234
```

In [10]:
```
PubKey = (n, e)
PrivKey = d
PubKey, PrivKey
```

Out[10]:
```
((1769735130712184081, 405337480659039757), 670234520228330293)
```

In [ ]:
```

```