In [3]:

```
p = next_prime(2^32)
Zp = IntegerModRing(p)
```

In [4]:

```
aCE, bCE = 3199880891, 3090779858
E= EllipticCurve(Zp, (aCE, bCE))
E
```

Out[4]:

```
Elliptic Curve defined by y^2 = x^3 + 3199880891*x + 3090779858 over Ring o
f integers modulo 4294967311
```

In [6]:

```
ordem = E.order()
ordem
```

Out[6]:

```
4295028948
```

In [18]:

```
P = E(4015973431 , 1728469600)
P.order()
```

Out[18]:

```
4295028948
```

In [19]:

```
P
```

Out[19]:

```
(4015973431 : 1728469600 : 1)
```

In [20]:

```
a = randint(2,ordem)
a
```

Out[20]:

```
1694993099
```

In [21]:

```
Q = a*P
Q
```

Out[21]:

```
(2372295191 : 2691966054 : 1)
```

In [23]:

```
PubKey = (E, P, Q)
PubKey
```

Out[23]:

```
(Elliptic Curve defined by y^2 = x^3 + 3199880891*x + 3090779858 over Ring
of integers modulo 4294967311,
 (4015973431 : 1728469600 : 1),
 (2372295191 : 2691966054 : 1))
```

In [25]:

```
mens = (12, 34)
```

In [26]:

```
k = randint(2, ordem)
```

In [27]:

```
c0 = k*P
```

In [28]:

```
y1, y2, _ = k*Q
```

In [29]:

```
c1 = y1*mens[0]
c2 = y2*mens[1]
cifr = (c0, c1, c2)
cifr
```

Out[29]:

```
((3814314712 : 220907041 : 1), 2578733731, 1113269067)
```

In [30]:

```
Y1, Y2, _ = a*cifr[0]
```

In [31]:

```
M1 = cifr[1]*1/Y1
M2 = cifr[2]*1/Y2
M1, M2
```

Out[31]:

```
(12, 34)
```

In [0]:

```

```