In [1]:
```
p = random_prime(2^16, lbound=2^15)
p
```

Out[1]:
```
38453
```

In [2]:
```
Zp = IntegerModRing(p)
```

In [3]:
```
a = Zp.random_element()
b = Zp.random_element()
gcd(4*a^3+27*b^2, p) == 1
```

Out[3]:
```
True
```

In [4]:
```
E = EllipticCurve(Zp, [a, b])
E
```

Out[4]:
```
Elliptic Curve defined by y^2 = x^3 + 14634*x + 34145 over Ring of integers
modulo 38453
```

In [5]:
```
E.order()
```

Out[5]:
```
38714
```

In [9]:
```
P = E.random_element()
P, P.order()
```

Out[9]:
```
((38447 : 37989 : 1), 38714)
```

In [10]:
```
priv_key = randint(2, P.order()-1)
priv_key
```

Out[10]:
```
20548
```

In [11]:
```
Q = priv_key*P
```

In [12]:
```
pub_key = (E, P, Q)
pub_key
```

Out[12]:
```
(Elliptic Curve defined by y^2 = x^3 + 14634*x + 34145 over Ring of integer
s modulo 38453,
 (38447 : 37989 : 1),
 (5647 : 15403 : 1))
```

In [13]:
```
Mens = E.random_element()
Mens
```

Out[13]:
```
(18048 : 15117 : 1)
```

In [14]:
```
k = randint(2, P.order()-1)
cifr = (Mens+k*Q, k*P)
cifr
```

Out[14]:
```
((9757 : 14419 : 1), (12994 : 22089 : 1))
```

In [15]:
```
decifr = cifr[0]-priv_key*cifr[1]
decifr
```

Out[15]:
```
(18048 : 15117 : 1)
```

In [ ]:
```

```