In [3]:
```
p = next_prime(2^16)
q = next_prime(2^15)
n = p*q
```

In [4]:
```
p, q, n
```

Out[4]:
```
(65537, 32771, 2147713027)
```

In [5]:
```
Zn = IntegerModRing(n)
```

In [19]:
```
x, y = Zn(12), Zn(34)
```

In [20]:
```
a = Zn.random_element()
b = y^2-x^3-a*x
gcd(4*a^3+27*b^2, n) == 1
```

Out[20]:
```
True
```

In [21]:
```
En = EllipticCurve(Zn, (a, b))
En
```

Out[21]:
```
Elliptic Curve defined by y^2 = x^3 + 394569140*x + 1708308829 over Ring of intege
rs modulo 2147713027
```

In [25]:
```
M = En(x, y)
M
```

Out[25]:
```
(12 : 34 : 1)
```

In [26]:
```
Ep = EllipticCurve(GF(p), (a, b))
Eq = EllipticCurve(GF(q), (a, b))
```

In [27]:
```
Ep
```

Out[27]:
```
Elliptic Curve defined by y^2 = x^3 + 36400*x + 21387 over Finite Field of size 65
537
```

In [28]:
```
o_Ep = Ep.order()
o_Eq = Eq.order()
```

In [33]:
```
e = randint(2, min(o_Ep, o_Eq))
e
```

Out[33]:
```
21037
```

In [34]:
```
gcd(e, o_Ep) == 1, gcd(e, o_Eq) == 1
```

Out[34]:
```
(True, True)
```

In [35]:
```
d = power_mod(e, -1, lcm(o_Ep, o_Eq))
d
```

Out[35]:
```
17411173
```

In [36]:
```
pub = (n, a, b, e)
```

In [37]:
```
M
```

Out[37]: (12 : 34 : 1)

In [39]:
```
Q = d*M
Q
```

Out[39]: (349754044 : 1811305145 : 1)

In [40]:
```
e*Q
```

Out[40]: (12 : 34 : 1)

In [41]:
```
e*Q == M
```

Out[41]: True

In [0]:
```

```