In [1]:

```
p = random_prime(2^16, lbound=2^15)
q = random_prime(2^16, lbound=2^15)
p % 3 == 2 and q%3 == 2
```

Out[1]:

```
False
```

In [3]:

```
while not(p % 3 == 2 and q%3 == 2):
    p = random_prime(2^16, lbound=2^15)
    q = random_prime(2^16, lbound=2^15)
```

In [4]:

```
p, q
```

Out[4]:

```
(52379, 3221)
```

In [5]:

```
n = p*q
```

In [6]:

```
Nn = lcm(p+1, q+1)
Nn
```

Out[6]:

```
9376020
```

In [7]:

```
e = randint(2, Nn)
gcd(e, Nn) == 1
```

Out[7]:

```
True
```

In [8]:

```
while gcd(e, Nn) != 1:
    e = randint(2, Nn)
e
```

Out[8]:

```
953251
```

In [9]:

```
d = power_mod(e, -1, Nn)
d
```

Out[9]:

```
6747511
```

In [10]:

```
PubKey = n, e
Priv = d
```

In [11]:

```
mx, my = 12, 34
```

In [12]:

```
Zn = IntegerModRing(PubKey[0])
```

In [13]:

```
b = Zn(my^2-mx^3)
b
```

Out[13]:

```
168712187
```

In [14]:

```
En = EllipticCurve(Zn, (0, b))
En
```

Out[14]:

```
Elliptic Curve defined by y^2 = x^3 + 168712187 over Ring of integers modulo 16871
2759
```

```
In [15]: cifr = e*En(mx, my)
         cifr
```

```
Out[15]: (7970971 : 159118044 : 1)
```

```
In [16]: Priv*cifr
```

```
Out[16]: (12 : 34 : 1)
```

```
In [0]:
```