In [1]:
```
p = next_prime(2^32)
p
```

Out[1]:
```
4294967311
```

In [2]:
```
Zp = IntegerModRing(p)
a = Zp.random_element()
b = Zp.random_element()
```

In [3]:
```
E = EllipticCurve(Zp, [a, b])
E
```

Out[3]:
```
Elliptic Curve defined by y^2 = x^3 + 1615520460*x + 309802741 over Ring of
integers modulo 4294967311
```

In [4]:
```
N = E.order()
N
```

Out[4]:
```
4295092842
```

In [5]:
```
epsilon = N-p-1
epsilon
```

Out[5]:
```
125530
```

In [6]:
```
floor(2*sqrt(p))
```

Out[6]:
```
131072
```

In [7]:
```
k = 30
mens = 1234
x= mens*k
while legendre_symbol(x^3+a*x+b, p) != 1:
    x = x+1
y = sqrt(x^3+a*x+b)
P = E(x, y)
P
```

Out[7]:
```
(37024 : 385739947 : 1)
```

In [8]:
```
Z_N = IntegerModRing(N)
```

In [9]:
```
e_A = Z_N.random_element()
while gcd(e_A, N) != 1:
    e_A = Z_N.random_element()
d_A = 1/e_A
e_A, d_A
```

Out[9]:
```
(3800356099, 2098654501)
```

In [10]:
```
e_B = Z_N.random_element()
while gcd(e_B, N) != 1:
    e_B = Z_N.random_element()
d_B = 1/e_B
e_B, d_B
```

Out[10]: (3391624379, 2088925763)

In [13]:
```
passo1 = ZZ(e_A)*P
passo1
```

Out[13]: (3473090761 : 903265494 : 1)

In [14]:
```
passo2 = ZZ(e_B)*passo1
passo2
```

Out[14]: (2791040269 : 2652849080 : 1)

In [15]:
```
passo3 = ZZ(d_A) * passo2
passo3
```

Out[15]: (2386909762 : 1632959392 : 1)

In [16]:
```
passo4 = ZZ(d_B)*passo3
passo4
```

Out[16]: (37024 : 385739947 : 1)

In [19]:
```
decifr = floor(ZZ(passo4[0])/k)
```

In [20]:
```
decifr
```

Out[20]: 1234

In [ ]:
```

```