Elliptic Curve Key Pair Generation

How Bitcoin creates public/private keys

1. Generate Random

256-bit number

(CSPRNG)

2. Private Key (k)

256 bits

KEEP SECRET!

3. EC Point Multiply

`K = k * G`

G = generator point

4. Public Key (K)

(x, y) coordinates

Can share freely

secp256k1 Curve Parameters

```
p = 2^256 - 2^32 - 977 (prime)

a = 0, b = 7

y^2 = x^3 + 7 (mod p)

Order n = ~2^256
```

One-Way Function:

K = k*G is easy, but finding k from K is infeasible

Source: SEC 2: Recommended Elliptic Curve Domain Parameters (Certicom)