P ~~> 160-bits~~ prime number

p -> n_b bits

2^(n_b/2) operations

Miller-Rabin Primality Test Algorithm -> polynomial time (randomized algorithm)

n^2, n^3 ...

n = 13

n-1 = 12 = 2^2.3, k = 2, q = 3

select a and b from Z_p = {0, 1, 2, ..., p-1} such that 4a^3 + 27b^2 #0 (mod p)

one-way function h(·) ->

G = (2, 7)
h(2 || 7) = 20

|| - > concetenation operator

h(1000 || 1101) = h(10001101) = 30

We call **G** is a base point in E_p(a,b) of order n if n.G = G + G + ... + G (n times) = O, point at infinity or zero point

Security Class (Sci) -> base point Gi, full (secret) key ski and partial (subsecret) key si

Security Class (Scj) -> base point Gj, full (secret) key skj and partial (subsecret) key sj

Sck >= Scj: (x- h(x_k,j || y_k,j)) where sk.Gj = (x_k,j, y_k,j)

Scj has a secret message: MSG =”Meet me after new year party at 10:30 AM at Stadium”

Scj -> *: E_Skj[MSG]

Sci: D_Skj[**E_Skj[MSG]] = MSG.**