

ECDH_PHASE_BB_BIGD

Application for compute the generator,
select a secret key from
pseudo-random number and compute
a point for sharing.

Input values: MOD , a , b

Output values: x_k , y_k (stored in array)

Subfunctions:

TheFirstPointBIGD

SecretKeyBIGD

PointCompBIGD

call TheFirstPointBIGD

call SecretKeyBIGD

Value alignment

$iterator = SecKey$ (copy value)

$iterator += 1$ (increase value due the first position is
occupied by the first point)

call PointCompBIGD

Stored results in
array