

## ECDH\_PHASE\_BA\_BIGD

Aplication for select a secret key from psudo-random number and compute a point for sharing.

Input values: *Order, Xf, Yf, a, MOD*

Output values: *ResultX, ResultY*

### Subfunctions:

SecretKeyBIGD

PointCompBIGD

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