



$$K1 = g^{BE1} \bmod p$$

$$K2 = g^{BE2} \bmod p$$