αq≡(g(p1)/q) q (mod p) ≡g(p1) (mod p) ≡1(mod p)

所以α的次数l|q。

已知αl≠1(mod p)，

所以α的次数为q。

------------------------------------

s1≡k1(h(m1)a r) mod (p)、

s2≡k1(h(m2)a r) mod (p)，

则s1s2≡ k1(h(m1)h(m2)) mod (p)。

若(s1s2, p1)=1，

则k≡ (s1s2)1(h(m1)h(m2)) mod (p)。

根据k可计算出a。

-----------------------------

。

因为

，

所以

，

所以

。