Subject: [Fwd: RE: Minding our Ps and Qs in Dual_EC]

Date: Wednesday, October 27, 2004 at 12:09:25 PM Eastern Daylight Time

From: John Kelsey

To: larry.basham@nist.gov

---------- Original Message ----------
Subject: RE: Minding our Ps and Qs in Dual_EC
From: "Don Johnson" <DJohnson@cygnacom.com>
Date: Wed, October 27, 2004 11:42 am
To: "John Kelsey" <john.kelsey@nist.gov>

John,

P = G.
Q is (in essence) the public key for some random private key.

It could also be generated like a(nother) canonical G, but NSA kyboshed this idea, and I was not allowed to publicly discuss it, just in case you may think of going there.

Don B. Johnson

-----Original Message-----
From: John Kelsey [mailto:john.kelsey@nist.gov]
Sent: Wednesday, October 27, 2004 11:17 AM
To: Don Johnson
Subject: Minding our Ps and Qs in Dual_EC

Do you know where Q comes from in Dual_EC_DRBG?

Thanks,

-John

Subject: Minding our Ps and Qs in Dual_EC

Date: Wednesday, October 27, 2004 at 11:16:39 AM Eastern Daylight Time

From: John Kelsey

To: Don Johnson

Do you know where Q comes from in Dual_EC_DRBG?

Thanks,

-John