

Re: Problems With Public Key Cryptosystems

Source: <http://sci.tech-archive.net/Archive/sci.math/2004-07/3688.html>

From: David A. Scott (daVvid_a_scott_at_email.com)

Date: 07/14/04

Date: 14 Jul 2004 17:54:05 GMT

daw@taverner.cs.berkeley.edu (David Wagner) wrote in
news:cd3mef\$2j6t\$1@agate.berkeley.edu:

>
> *Actually, the number of conditions is shrinking. The bit about safe*
> *primes, small divisors of $p-1$, etc., is now considered irrelevant; they*
> *seem to have been an artifact of the old factoring algorithms. Today's*
> *best factoring algorithms don't care whether $p-1$ has small factors, so*
> *the advice today is just to generate a pair of primes uniformly at*
> *random without worrying about special conditions.*
>
>

Two questions who says the conditions are shrinking. There could be groups eager to decode public keys so they promote the idea of using less conditions. Secondly how does one guarantee that one is picking a random pair of primes uniformly since for one thing the distribution of primes is not random just look at distribution of twin primes and such.

David A. Scott

--
My Crypto code
<http://bijective.dogma.net/crypto/scott19u.zip>
<http://www.jim.com/jamesd/Kong/scott19u.zip> old version
My Compression code <http://bijective.dogma.net/>
**TO EMAIL ME drop the roman "five" **
Disclaimer: I am in no way responsible for any of the statements
made in the above text. For all I know I might be drugged.
As a famous person once said "any cryptographic
system is only as strong as its weakest link"