

Re: Problems With Public Key Cryptosystems

Source: <http://sci.tech-archive.net/Archive/sci.math/2004-07/3696.html>

From: Tom St Denis (tom_at_securescience.net)

Date: 07/14/04

Date: Wed, 14 Jul 2004 18:02:44 GMT

David A. Scott wrote:

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

Well that would be because the GNFS which does in fact work [and so does the QS] are faster than the Rho method on which that would depend.

> *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.*

Generating uniformly random primes is not as hard as you think it is.

1. Generate a totally random number [ok random as in from a secure PRNG]
2. Test for primality, repeat as required.

The issue of "distribution" arose from systems that worked as

1. Generate random integer N
2. Test it, if it's not prime $N = N + 2$, goto 2
3. return N

sci.math: Re: Problems With Public Key Cryptosystems

And yes, that does skew to some primes over others.

The first approach is equivalent to saying with a random 16-bit value pick a uniformly random value in 1-40000. Well how do you do that?

1. $N = \text{rand}()$
2. If $N < 1$ or $N > 40000$ goto 1
3. return N

since the span 0..65535 is uniform the sub-span 1-40000 must also be uniform.

Tom