

Re: [Newbie] Prime factorization question

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/0853.html>

From: Bill Unruh (unruh_at_string.physics.ubc.ca)

Date: 10/08/03

Date: Wed, 8 Oct 2003 10:30:35 +0000 (UTC)

Mxsmanic <mxsmanic@hotmail.com> writes:

]Lorenzo Bolognini writes:

]> So they are known and sure they are proven and certificated primes
]> (otherwise the cipher would be vulnerable to other attacks than plain
]> bruteforcing) and they are finite so the number of possible primes that may
]> generate the cipher is very much restricted...

]PGP selects prime numbers at random from the set of all prime numbers
]with appropriate lengths ($n/2$, where n is the desired length of the
]modulus). The number of primes at any given length is indeed finite,
]but it is very, very large for any modulus of the common sizes used in
]PGP (384 bits and up), and so there is no real risk of the same primes
]being selected for two different keys.

]The primality of the selected random numbers is not conclusively
]verified, but it is tested with an algorithm that provides a very high

While true, it now could be. There is a recent algorithm which can prove
conclusively that a number is prime or not.

PGP could now use that. It would make no difference.

]degree of certainty with respect to their primality (additionally, if p
]and q are not both prime, typically the encryption will fail in a fairly
]obvious way quite quickly).

]> well how many are they?

]For a 1024-bit modulus, you need two 512-bit primes. If I remember
]correctly, there are probably about 4×10^{151} primes of that length or
]less. So even with a 1024-bit modulus, we will never run out of unique
]primes, and the possibility of getting two identical primes is, for all
]practical purposes, zero.

]I do wonder how many primes there are of exactly n bits, but I'm not

The approximation (quite good) is $2^n / (n \ln(2))$

sci.crypt: Re: [Newbie] Prime factorization question

]sure how to calculate or estimate that. Also, it's important that the
]primes be selected entirely at random.

Well, they are not. Primes which are far away from the next lower prime are selected preferentially by the algorithm used. (Ie, if prime p_i is the i th prime, then p_i is selected with a probability proportional to $p_i - p_{(i-1)}$). Thus a prime which is say 20 away from the next lower prime will be selected with 10 times the probability as one for which the next lower prime is only 2 away.

However, I do not believe that anyone knows how to use this fact to aid in the factoring.