

Re: prime numbers?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-08/0095.html>

From: Jeremy Bishop (*requiem_at_org.praetor*)

Date: 08/10/03

Date: Sat, 09 Aug 2003 21:00:31 -0700

PCportinc wrote:

>> *In fact, from what I know, the largest prime number has less
>> than 1,000,000 digits.*
>
> *ok, but why is that important in cryptography and how are prime numbers
> used?*
>
> *so 1, 2, 3, 5, 7, 11, 13, 17, 19 are prime?*
> *except for 2, the rest are odd.*

1 is not considered prime; the reason are given in the FAQ of the previously linked website.

When talking about primes in reference to cryptography, it is usually also in reference to the RSA public key algorithm. Here's a good explanation: <http://www.muppetlabs.com/~breadbox/txt/rsa.html>

The short answer to your question is that two primes (we'll call them U and V) are used when generating the public and private keys. At one point, they are multiplied together, and this number (call it R) is incorporated into both the public and private key. (Yes, this is necessary for the process to work.) To break RSA, you must recover those two primes, and the only way to do that is to factor R (and if U and V are large enough, you won't be able to do that in any reasonable amount of time).

--

Exclusive dedication to necessitious chores without interludes of hedonistic diversion renders John a hebetudinous fellow.