

Re: Good enough for crypto?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-11/1971.html>

From: Scott Wilber (swilber_at_comscire.com)

Date: 11/28/03

Date: 27 Nov 2003 15:41:31 -0800

Paul Crowley <paul@JUNGCATCHER.ciphergoth.org> wrote in message news:<87fzgbbl73.fsf@saltationism.subnet.hedonism.cluefactory.org>...

> swilber@comscire.com (Scott Wilber) writes:

>> *I find it quite boring when someone posts a response merely for the*

>> *purpose of attacking. This may be entertaining for them, but it is*

>> *just a waste of time for most people. I will attempt to make a*

>> *reasonable reply anyway.*

>

> *This is very enlightening. I've wondered for a while whether the*

> *ComScire generators were good, but haven't had time to do a detailed*

> *investigation. Fortunately the way the manufacturers respond to*

> *expert technical criticism is the best determiner there is of snake*

> *oil.*

>

> *Clue: When someone like GGR criticises you, you start by thanking him*

> *for taking the time to examine your design.*

Fortunately, the government and military agencies and large companies around the world that have been using our generators for the past 8 years do not agree with your amazing powers of evaluation.

See for example:

<http://www-106.ibm.com/developerworks/library/s-beating.html>

"Several hardware devices for generating random numbers are commercially available. Probably the most widely used device is the ComScire QNG..."

"...An unbiased review of this generator by Robert Davies (see Resources) claims that it 'seems to be the only generator specifically designed for statistical purposes and where the manufacturer has made a real effort to understand the effect of bias and correlation on the numbers that are finally produced'."

<http://www.rsasecurity.com/rsalabs/challenges/factoring/faq.html>

"The RSA challenge numbers were generated using a secure process that guarantees that the factors of each number cannot be obtained by any method

other than factoring the published value. No one, not even RSA

sci.crypt: Re: Good enough for crypto?

Laboratories,
knows the factors of any of the challenge numbers.

The generation took place on a Compaq laptop PC with no network connection

of any kind. The process proceeded as follows:

1) First, 30,000 random bytes were generated using a ComScire QNG hardware random number generator..."

http://en2.wikipedia.org/wiki/Hardware_random_number_generator

"Manufacturers of random number generator devices:

ComScire (Popular with military cryptographers, it's said, and very fast)..."

If you search, you will find other references. However, we never reveal any of our customers (unless they have already made a public disclosure) or how many devices are in use, since most are used in security and cryptographic applications including satellite security.

Scott Wilber
ComScire – Quantum World Corporation