

Re: encryption with pi

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-07/1444.html>

From: Phil Carmody (*thefatphil_demunged_at_yahoo.co.uk*)

Date: 07/31/04

Date: 31 Jul 2004 03:01:55 +0300

pubkeybreaker@aol.comstuff (Bob Silverman) writes:

> *Sigh.*

Agreed.

> *I get tired of this. I am competent to judge.*

Agreed.

> *The proposed cipher is easily broken.*

Agreed.

> *Computing the
> n'th digit of Pi can be done in constant time
> (without computing prior values) by an algorithm of
> Simon Plouffe.*

Borwein, Bailey and Plouffe claim the algorithm "scale[s]
nearly linearly with the order of the digit desired".

(That's from the abstract of their paper. The Bellard
improvements are simply a multiplicative constant, not
a change in Big-Oh)

> *The algorithm is quite fast.*

>

> *Even if it were not constant time, generating 100*

> *million digits of Pi is TRIVIAL.*

Agreed.

> *I suggest searching the literature next time before*

> *shooting your mouth off. You do know how to do*

> *a Web search, don't you?*

Funnily enough, about 75% of my bookmarks for BBP are now
dead links.

sci.crypt: Re: encryption with pi

Phil

--

1st bug in MS win2k source code found after 20 minutes: scanline.cpp
2nd and 3rd bug found after 10 more minutes: gethost.c
Both non-exploitable. (The 2nd/3rd ones might be, depending on the CRTL)