

## Re: encryption with pi

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-07/1389.html>

---

**From:** Jeff Williams ([frostback\\_at\\_canada.com](mailto:frostback_at_canada.com))

**Date:** 07/30/04

Date: Thu, 29 Jul 2004 20:23:12 -0500

Tom St Denis wrote:

> [vedaal@hush.com](mailto:vedaal@hush.com) wrote:

>

>

>>can the following simple substitution cipher using pi, be made secure

>>?

>>

>> $C = P \text{ rot } [ s(l+n) \text{ mod } 256 ]$

>>

>>where 's' is a substring of pi of length k, beginning at digit 'l',

>>and 'n' is the sequenced character of the plaintext

>

>

> <snip>...

>

> What does "rot" mean anyways?

>

> That aside... finding digits of Pi is **\*\*SLOW\*\*** and consumes a heck lot of  
> memory. That and who says identifying a sequence as part of "Pi" is a hard  
> problem? Who knows there may be a sub-exponential algorithm that given L  
> digits of pi you can determine where the first one was.

>

> Alternatively who says given L digits of Pi you can't predict the next with  
> more than uniform probability?

>

> Quite frankly the idea is a bit short sighted. It's inefficient and has no  
> provable properties other than it's not a simple pattern.

>

> Tom

>

>

Rot = rotate. Off-colour posts used to be (haven't seen any recently)  
"encrypted" with rot 13 – Caesar cipher with a key of 13.

I've never heard of anyone showing a pattern in the digits of PI (not to say there are no patterns). Assuming (big assumption) there is no discernable pattern, using a sequence of the digits of PI as a basis of (I hate to say it) an OTP MIGHT work.

sci.crypt: Re: encryption with pi

As Tom noted, very slow generation of digits of PI. Also, the number of known digits of PI yields a very small (in modern terms) keyspace. Even worse, the effort to calculate the  $n+1$ th digit of PI is greater than the effort to calculate the  $n$ th digit of PI.

It's simple. It's elegant. It may be theoretically secure. But it's thoroughly impractical.

Don't know how many others thought of this concept. It occurred to me somewhere around 1979 (about the time I got my driver's licence).

Jeff