

## Re: encryption with pi

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-07/1408.html>

---

**From:** Tom St Denis ([tomstdenis\\_at\\_iahu.ca](mailto:tomstdenis_at_iahu.ca))

**Date:** 07/30/04

Date: Fri, 30 Jul 2004 12:57:22 GMT

vedaal@hush.com wrote:

> *Jeff Williams* <[frostback@canada.com](mailto:frostback@canada.com)> wrote in message

> *news:<aphOc.3553\$K5.16220@news1.mts.net>...*

>> *Tom St Denis* wrote:

>

>>> *That aside... finding digits of Pi is **\*\*SLOW\*\*** and consumes a heck lot  
>>> of memory.*

>

> *agreed,*

> *from scratch, very slow,*

> *but since pi has already been calculated up to 200 billion places,*

> *and can simply be stored on disk,*

> *which it has been for 100 million digits,*

> *it is now very fast,*

IIRC this is the "Maurer Stream Cipher" where you have huge public sources of data. Schneier [et al] have attack it and variants [using multiple points in the stream].

Besides, storing 100MB to encrypt a small message is just inefficient.

Tom