

sci.crypt: Re: Rate the following Cryptolibraries from fastest to slowest

Re: Rate the following Cryptolibraries from fastest to slowest

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-07/2220.html>

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

Date: 07/31/03

Date: Thu, 31 Jul 2003 11:43:49 +0300

On Thu, 31 Jul 2003 10:01:43 +0200, George Joseph wrote:

- > *Please rate the following libraries from fastest to slowest (the pure*
- > *C-implemented version – not assembler)?*
- > *(a) MIRACL*
- > *(b) LibTomMath*
- > *(c) GMP*
- > *(d) LIP*
- >
- > *If there are any others which you think are faster, please inform of them*
- > *and where I can obtain them.*

They probably won't be faster than GMP, but you're missing bn, Piologie, and NTL, for a start. If GMP does what you want natively, then I'd stake my that on GMP being faster than anything else.

Why don't you just download them, compile them, and speed test them yourself?

Phil