

Re: Assembler versus ANSI C

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-07/2237.html>

From: Bryan Olson (*fakeaddress_at_nowhere.org*)

Date: 07/31/03

Date: Thu, 31 Jul 2003 11:56:28 GMT

George Joseph wrote:

- > *I would like to know whether or not it will be worth the while to compute*
- > *the time required to compute an RSA encryption/decryption, DH key*
- > *exchange,*
- > *El-Gamal/DSA signature with different expmod & modmul techniques in*
- > *ANSI C,*
- > *and obtain a comparison in terms of time and iterations needed by the*
- > *Public-key cryptosystems(PKC).*
- >
- > *Or is it more beneficial to use assembler and optimise every step to*
- > *see how*
- > *they compare to each other. The emphasis of this task is not to see how*
- > *quickly each PKC is implemented, but rather how each PKC compares to the*
- > *other using the same programming platform(whether it be assembler or C).*
- >
- > *So must I write the PKC algos in C or assembler?*

Are you sure you want to write them yourself? You may be a fine programmer, but people have put a lot of work into writing fast public-key crypto code. It would take a huge amount of work to write your own implementations that are as fast as any out there.

The speed of an algorithm in a particular language is defined by the fastest such implementation. If you compare slower code, then the results are not significant.

I'd suggest surveying implementations already out there.

--

--Bryan