

Re: Successful remote AES key extraction

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/1120.html>

From: D. J. Bernstein (*djb_at_cr.yp.to*)

Date: 04/17/05

Date: Sun, 17 Apr 2005 08:41:57 +0000 (UTC)

BRG wrote:

> *I am simply pointing out that in comparing the speed of your assembler
> code with the speed of other people's C code you are not comparing like
> with like.*

Speed is speed. I'm simply reporting all the timings I found; I'm not excluding any particular programming language. When I say that your AES code reportedly takes 482 Pentium-III cycles (202 for expansion, 280 for encryption), I'm making no comments about how that speed was achieved.

If someone wants to explain bad performance or timing leaks by saying "I decided to use C and couldn't do better in C," that's useful data for implementors choosing programming tools. But saying "I decided to use C and it's unfair to be compared to asm" is silly.

Anyway, all I was saying was that the published aes_ppro code takes 23 Pentium III cycles per round with compressed tables, and nobody claims that uncompressed tables can do better than 20 cycles, so obviously there's not a serious slowdown from compressed tables. In fact, I see no reason to disbelieve Agner Fog's statement that there's zero penalty for arbitrary alignment within lines on the PPro/PPIII.

---D. J. Bernstein, Associate Professor, Department of Mathematics,
Statistics, and Computer Science, University of Illinois at Chicago