

comp.unix.solaris: Re: Bug in Sun compiler WS6U2? – Crashes during compile phase with–fast.

## Re: Bug in Sun compiler WS6U2? – Crashes during compile phase with–fast.

**Source:** <http://unix.derkeiler.com/Newsgroups/comp.unix.solaris/2005-03/2040.html>

---

**From:** Logan Shaw (*lshaw-usenet\_at\_austin.rr.com*)

**Date:** 03/24/05

Date: Thu, 24 Mar 2005 01:20:57 GMT

Dave wrote:

> *Logan Shaw wrote:*

>> *However, you can factor large*

>> *numbers that are the product of two primes, and if you did that, it'd*

>> *be a bad thing for cryptography as we know it.*

> *But it can factor a composite number consisting of two similar sized*  
> *primes virtually instantly.*

>

> *In[10]:= 2760727302559 \* 2760727302517 // multiple two primes.*

>

> *Out[10]= 7621615238978741781241003 // get the result*

>

> *In[11]:= FactorInteger[7621615238978741781241003] // factor it*

>

> *Out[11]= {{2760727302517, 1}, {2760727302559, 1}} // The two prime factors.*

That Mathematica can do that nearly instantaneously is pretty impressive.

As far as I know, the only way to do this is to just brute force it by dividing by numbers from 2 .. floor(sqrt(7621615238978741781241003)) until you get one that comes out evenly.

Actually, you can do a little better than that by using simple tests to see if the number is a multiple of 2, 3, 5, etc. That allows you to skip about 75% of the brute force divisions, but that only makes your code something like 4 times as fast, which is not that much!

You still have to do something like 700 billion divisions to find that, unless there is some optimization technique that I am missing something.

Which actually there must be unless your copy of Mathematica is running on some massively parallel computer with hundreds of ~1 GHz processors...

By the way, I think there are other methods of cryptography that

comp.unix.solaris: Re: Bug in Sun compiler WS6U2? – Crashes during compile phase with–fast.

don't involve prime numbers, but I'm not aware of any methods of public/private key cryptography that don't use prime numbers. Not to say that they don't exist, but I'm not aware of them.

– Logan