

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/2005-03/2036.html>

---

*From:* Dave ([nospam\\_at\\_nowhere.com](mailto:nospam_at_nowhere.com))

*Date:* 03/24/05

Date: Thu, 24 Mar 2005 00:31:15 +0000

Logan Shaw wrote:

> *David Kirkby wrote:*

>

>> *Now if someone can find a fast way of factoring large prime numbers,*

>> *that will be the end of ssh as it is currently known.*

>

>

> *Now you're correctly quoting Bill Gates's famous incorrect statement*

> *about cryptography.*

Believe it or not, I found on Mathworld

<http://mathworld.wolfram.com/PrimeNumber.html>

today that thing Gates said, found it funny and sent an email around at work to a few who I thought would find it funny too. Not realising I'd put an identical silly statement on a newsgroup the night before!!

I'd like to say its an easy mistake to make (to excuse me), but I will not, as then it would excuse Bill Gates, who I rather dislike.

Yes, I know you can't factor primes – by definition. What I meant of course is that if there was found a way of factorising large composite numbers, it would be the end of cryptography. I'm sure there are cryptographic techniques that don't use primes.

> *You can't factor large \*prime\* numbers, because*

> *you can't factor \*any\* prime numbers. 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.*

I'm sure one day someone will come up with a general formula for finding the nth prime, which would go a long way towards making factorisation of huge composite numbers. Mathematica takes about 45 seconds to find the 100000000000th prime on my computer.

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

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

```
In[8]:= Prime[100000000000] //Timing
```

```
Out[8]= {44.51 Second, 2760727302517}
```

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.
```