

Re: triple algorithms

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2008-02/msg00959.html>

- *From:* Ertugrul Söylemez <es@xxxxxxxx>
 - *Date:* Thu, 28 Feb 2008 18:32:47 +0100
-

On Thu, 28 Feb 2008 17:26:23 +0000

Guy Macon <<http://www.guymacon.com/>> wrote:

I see one reason to trust AES more than BBS. We already have a polynomial-time factoring algorithm, so we know that it's possible. We just don't have the computer to run it.

If you mean Shor's algorithm, we certainly don't know that it's possible.

How come?

It requires a computer that may or may not be possible.

If you are curious as to why, do a web search on "Quantum Computers"

That's what I was saying. We know that factorization can be done in polynomial time. We just don't have the computer to do it.

Regards,
Ertugrul.

—

<http://ertes.de/>

.