

Re: JSH: Easy math, easy solution

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-02/2952.html>

From: Steven (*somewherenonexistent_at_yahoo.com*)

Date: 02/09/05

Date: 9 Feb 2005 05:26:40 -0800

>Factorization is quite simple. Here is an algorithm for it.

>Input: a composite number n .

>Output: an ordered pair (b,c) such that $1 < b < n$, $1 < c < n$, and $bc = n$.

Why on earth did you post this!!! IF YOU THINK FACTORIZATION IS SO EASY TRY FACTORING A 500+ DIGIT RSA MODULUS!! Then tell us how easy it is to win the RSA factoring challenge. According to your reasoning, the trial-division algorithm is even *simpler**, but it is as slow as heck. The algorithm you posted (Pollard?) is only marginally better than trial-division, and unless I am mistaken, the algorithm is probabilistic, meaning it is possible (but not likely) to never return. Do I need you to tell me that some factorization *ALGORITHMS** are simple? I did a whole research paper on it!!!