

Re: Speculative, but at least interesting

Source: <http://sci.tech-archive.net/Archive/sci.physics/2004-09/3109.html>

From: Uncle Al (UncleAl0_at_hate.spam.net)

Date: 09/07/04

Date: Tue, 07 Sep 2004 08:01:46 -0700

Sam Wormley wrote:

>

> *Long Standing Math Puzzle May be Solved*

> http://www.guardian.co.uk/uk_news/story/0,3604,1298728,00.html

"if somebody really has cracked the so-called Riemann hypothesis, financial disaster might follow. Suddenly all cryptic codes could be breakable. No internet transaction would be safe."

Assume the Riemann hypothesis is true, then crack every code. A valid proof would alter nothing here. NSA can brute force crack any Officially sanctioned encryption right now. Being able in theory to factor the product of large primes isn't the same as actually doing it.

Eudora passwords are trivially cracked – your ISP account is naked. PKZIP encryptions are demonstrated crackable if you know some contained text.

MS Word and Word Perfect encryptions are easily crackable.

The DES is an NSA joke.

Recent versions of PGP are rumored to include an NSA back door.

What would change?

--

Uncle Al

<http://www.mazepath.com/uncleal/>

(Toxic URL! Unsafe for children and most mammals)

<http://www.mazepath.com/uncleal/az.pdf>