

Re: RSA algorithm

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-07/0387.html>

From: Michael Amling (*nospam_at_nospam.com*)

Date: 07/06/03

Date: Sun, 06 Jul 2003 14:36:19 GMT

vicky wrote:

> *Any idea?*

>

> *Suppose that the public key of RSA is (n, e) and $C = M^e \pmod n$. An*

> *algorithm A can invert 1% of the inputs in form $y = M^e \pmod n$. Prove*

> *that using algorithm A we can invert every input with high*

> *probability.*

> *Thank you :)*

Are you doing lakis's homework?

—Mike Amling