

Re: RSA: more than one secret exponent d exists ???

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-06/msg00340.html>

- *From:* Sebastian Gottschalk <seppi@xxxxxxxxxx>
 - *Date:* Tue, 06 Jun 2006 13:44:26 +0200
-

Kristian Gjøsteen wrote:

Sorry. I'll try to sketch the argument below, with as little mathematics as possible.
[...]

Still too complicated. Why not the easy way with some algebra?

The ring Z_n is a multiplicative composition of the mutually exclusive rings Z_p and Z_q (with respect to multiplication). The relation between e and d exists in Z_n , therefore must also exist in both Z_p and Z_q . Now if $m^{(d*e)}=m$ is true mod $(p-1)$ and mod $(q-1)$, you'll easily get that it must be true mod $\text{lcm}(p-1, q-1)$ as well.

This also shows that RSA can be applied to any finite fields and their composition, where the decomposition of the composite is a well-known hard problem.

.