

Re: doubts about rc4

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-11/1868.html>

From: Michael Amling (*nospam_at_nospam.com*)

Date: 11/26/03

Date: Wed, 26 Nov 2003 04:11:50 GMT

Gregory G Rose wrote:

> In article <Pine.GSO.4.58.0311251310330.22703@turmalina.dcc.ufmg.br>,

> Leonardo Barbosa e Oliveira <leob@dcc.ufmg.br> wrote:

>

>>Even though I am newbie about crypt., I think my results

>>are a little bit strangers. I am using avr studio simulator

>>for rc4. However, the number of cycles are varying as function

>>of both message size and key size.

>

> I don't know that this simulator is. But I do know

> that no-one has ever detected a cycle in RC4 if it

> was properly initialised.

I think the OP was talking about CPU cycles, rather than about repetitions in the keystream.

—Mike Amling