

doubts about rc4

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-11/1838.html>

From: Leonardo Barbosa e Oliveira (*leob_at_dcc.ufmg.br*)

Date: 11/25/03

Date: Tue, 25 Nov 2003 13:11:21 -0200

Dear Sirs!

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.

Concerning the first, I could not figure out what is happening, is it possible? cycles varying with message size?

About the last, at first, I found curious the fact that increasing key size the number of cycles used to decrease. Afterward, however, I realized the array has to be filled with the key size and, in turn, the more is the key size, the lesser is number of instructions to fill the array. Is that line of reasoning right?

Any help will be very appreciated.

Thanks in advance!

Regards,

Leonardo

"Não existe um caminho para a paz; a paz é o caminho"
Mahatma Gandhi