

Re: RC4, With Homebrew MAC...

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/2023.html>

From: Bartosz Zoltak (X_at_vmpcffunction.com;)

Date: 04/29/05

Date: Fri, 29 Apr 2005 00:20:21 +0200

Użytkownik <aweston@connectfree.co.uk> wrote:

- > *So, I ask. How about*
- > *multiplying each unencrypted byte, with the RC4 byte, and*
- > *checksumming*
- > *this value, to verify the packet has not been tampered with?*

If you think about RC4 and using *standard* algorithms is not your primary criteria, then you might use VMPC instead of RC4 and this way avoid many attacks against RC4. You would also have an already made dedicated MAC scheme with this cipher. If you like, you can find more information at www.VMPCfunction.com

Bartosz

--

Bartosz Zoltak

<http://www.vmpcfunction.com>

X@vmpcfunction.com; X=bzoltak