

Re: ANNOUNCE: Leopard10 CSPRNG

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-03/1976.html>

From: Bob Jenkins (bob_jenkins@burtleburtle.net)

Date: 03/24/03

From: bob_jenkins@burtleburtle.net (Bob Jenkins)

Date: 23 Mar 2003 17:34:52 -0800

mrsjunecarey@aol.com (Mrsjunecarey) wrote in message
news:<20030320130010.18805.00000103@mb-ct.aol.com>...

>

> (c) Robert Jenkins had a look over L9 and couldn't find a way to break it. L10

> has higher security than L9.

I didn't try to hard. I found a subset of the sequence I could detect bias in with DIEHARD and called it a night. I haven't found the motivation to look at L10. I've been off implementing something unrelated instead.