

NIST randomness-tests – EXE?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-09/2651.html>

From: Bartosz Zoltak ()_at_vmpcfunction.com)

Date: 09/30/03

Date: Tue, 30 Sep 2003 11:12:19 +0200

I would like to test the VMPC cipher also against the NIST battery of statistical tests, but did not manage to compile the C sources downloaded from <http://csrc.nist.gov/rng>

Does anybody have executables of those tests for PC? DOS or Windows version would be very helpful.

And are the tests worth running? Apart from the battery David Sexton proposed me, I have runded the Diehard tests and now have uploaded the results – at <http://www.vmpcfunction.com/c7.htm> I found it unclear how Diehard should be used – how many and how big files should be tested – I followed RSA's approach presented in RSA Labs Bulletin (No 8,1998) for BSAFE 3.x generator – and tested ten 11MB files with cipher output generted for different keys. At c7.htm I published the p-values generated by Diehard with average, minimal and maximal ones.

The NIST test suite seems not as popular as Diehard if I see right, could someone tell how valuable the NIST battery is?

--

Bartosz Zoltak
<http://www.vmpcfunction.com>
QPbzoltak@vmpcfunction.com
without "QP"