

## Re: Java encryption implementation

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-11/1042.html>

---

**From:** megagurka (megagurka\_at\_yahoo.com)

**Date:** 11/29/05

Date: 29 Nov 2005 04:02:25 -0800

TC wrote:

- > *There are several aspects of "random numbers" that are important in*
- > *cryptography. One of these is randomness. (If the generator produces*
- > *highly non-random results, this could help an attacker to crack it.)*
- > *But another one is /unpredictability/ – a completely different thing.*

Incorrect. Randomness and unpredictability are equivalent.

- > *Say you generate a huge number of sequential integers. That sequence of*
- > *integers is:*
- > *– randomly distributed (no integer appears more commonly than any other*
- > *one);*

Your sequence is not "randomly distributed".

- > *So my generator, which I offered as an instructive joke, was only meant*
- > *to illustrate that randomness is /not enough/, and having a long period*
- > *is also /not enough/. The numbers must also be /unpreictable/ – a*
- > *completely different thing.*

Of course randomness is enough for a RNG.

/JN