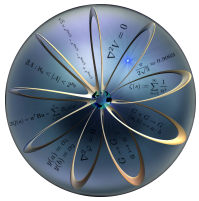

planetmath.org

Math for the people, by the people.

pseudorandom

Canonical name	Pseudorandom
Date of creation	2013-03-22 13:02:36
Last modified on	2013-03-22 13:02:36
Owner	Henry (455)
Last modified by	Henry (455)
Numerical id	8
Author	Henry (455)
Entry type	Definition
Classification	msc 68Q30
Classification	msc 60A99
Synonym	pseudorandom distribution ensemble
Synonym	pseudorandom ensemble

A distribution ensemble $\{D_n\}_{n\in\mathbb{N}}$ is *pseudorandom* if it is computationally indistinguishable from the ensemble $\{U_n\}_{n\in\mathbb{N}}$ where each U_n is the uniform distribution on the support of D_n. That is, no reasonable procedure can make meaningful predictions about what element will be chosen.