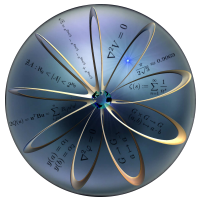

# planetmath.org

Math for the people, by the people.

## computationally indistinguishable

| | |
|---|---|
| Canonical name | ComputationallyIndistinguishable |
| Date of creation | 2013-03-22 13:03:11 |
| Last modified on | 2013-03-22 13:03:11 |
| Owner | Henry (455) |
| Last modified by | Henry (455) |
| Numerical id | 5 |
| Author | Henry (455) |
| Entry type | Definition |
| Classification | msc 68Q30 |

If $\{D_n\}_{n\in\mathbb{N}}$ and $\{E_n\}_{n\in\mathbb{N}}$ are distribution ensembles (on $\Omega$) then we say they are *computationally indistinguishable* if for any probabilistic, polynomial time algorithm $A$ and any polynomal function $f$ there is some $m$ such that for all $n > m$:

$$|\operatorname{Prob}_A(D_n) = \operatorname{Prob}_A(E_n)| < \frac{1}{p(n)}$$

where $\operatorname{Prob}_A(D_n)$ is the probability that $A$ accepts $x$ where $x$ is chosen according to the distribution $D_n$.