one-way function

Canonical name	OnewayFunction
Date of creation	2013-03-22 13:03:14
Last modified on	2013-03-22 13:03:14
Owner	Henry (455)
Last modified by	Henry (455)
Numerical id	7
Author	Henry (455)
Entry type	Definition
Classification	msc 68Q30
Synonym	one way function
Synonym	one-way
Synonym	one way

A function f is a *one-way function* if for any probabilistic, polynomial time computable function g and any polynomial function p there is m such that for all $n > m$:

$$\Pr[f(g(f(x))) = f(x)] < \frac{1}{p(n)}$$

where x has length n and all numbers of length n are equally likely.

That is, no probabilistic, polynomial time function can effectively compute f^{-1}.

Note that, since f need not be injective, this is a stricter requirement than

$$\Pr[g(f(x))) = x] < \frac{1}{p(n)}$$

since not only is $g(f(x))$ (almost always) not x, it is (almost always) no value such that $f(g(f(x))) = f(x)$.