

# Conjectured pseudorandom functions

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/2111.html>

---

*daidar3118\_at\_hotmail.com*

**Date:** 04/30/05

Date: 29 Apr 2005 16:41:03 -0700

What are the conjectured pseudorandom functions with arbitrary input length commonly used in practice? Is it necessary to choose the key of a pseudorandom function uniformly from the key space in order to ensure its randomness? Could we just feed the output of the pseudorandom function on an input  $x$  as the key to another pseudorandom function?