

## Re: Sun setting on stream ciphers?

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-02/2198.html>

---

**From:** Nicol So (*anonymous\_at\_no.spam.please*)

**Date:** 02/29/04

Date: Sun, 29 Feb 2004 14:37:09 GMT

Tom St Denis wrote:

- > *It's expected that a block cipher act like a PRP. A*
- > *stream cipher may be a PRF [e.g. it's time dependent too].*

A stream cipher does not behave like a pseudorandom function. Let  $m$  and  $m||m'$  be two plaintexts. Starting from identical initial states, a deterministic stream cipher  $E$  has the property that  $E(m, K)$  is a prefix of  $E(m||m', K)$ . A random function generally doesn't have this property.

--

Nicol So

Disclaimer: Views expressed here are casual comments and should not be relied upon as the basis for decisions of consequence.