

Re: Iterated Block Cipher versus Feistel

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-01/3047.html>

From: David Wagner (daw_at_taverner.cs.berkeley.edu)

Date: 01/31/05

Date: Sun, 30 Jan 2005 23:25:36 +0000 (UTC)

flip wrote:

>It appears that a Feistel cipher (like DES) is claimed different than an
>Iterated Block Cipher (IBC) like AES.

A Feistel cipher is a special kind of iterated block cipher.
All Feistel ciphers are iterated block ciphers, but not all
iterated block ciphers are Feistel ciphers.