

Iterated Block Cipher versus Feistel

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-01/3043.html>

From: flip (*flip_alpha_at_safebunch.com*)

Date: 01/31/05

Date: Sun, 30 Jan 2005 15:14:06 -0800

Hello,

I am having a difficult time finding out what the difference between the two definitions is.

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

Is there a subtle difference that I am missing between the two types?

They seem to basically use similar structures (rounds, key schedules and the like), so what does the distinction really say?

Sometimes I feel dense!