

sci.crypt: Re: Maybe we only need PCBC...

## Re: Maybe we only need PCBC...

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-06/1488.html>

---

*jsavard\_at\_ecn.ab.ca*

**Date:** 06/29/03

Date: Sun, 29 Jun 2003 14:32:55 GMT

jsavard@ecn.ab.ca wrote:

: I've restructured my page so that the more basic content on encryption  
: modes is no longer on a giant page about integrity-aware modes.

: So now the integrity-aware stuff is on

: <http://home.ecn.ab.ca/~jsavard/crypto/co040603.htm>

: and note that I haven't revised all the parent pages to include this in  
: their tables of contents yet.

I have further continued the process of separating useful content from  
useless content, to limit the maximum size of pages, by leaving the  
recognized integrity-aware encryption modes designed by others on that  
page, and putting my own fumbling attempts to design such a mode on

<http://home.ecn.ab.ca/~jsavard/crypto/co040604.htm>

John Savard