

## Re: Blockcipher >256 bit (for hardware implementation)

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-01/msg00659.html>

---

- *From:* Kristian Gjøsteen <[kristiag+news@xxxxxxxxxxxxx](mailto:kristiag+news@xxxxxxxxxxxxx)>
  - *Date:* Thu, 25 Jan 2007 07:55:00 +0000 (UTC)
- 

Mike Amling <[spamonly@xxxxxxxxxxxxx](mailto:spamonly@xxxxxxxxxxxxx)> wrote:

With no IV, the messages and ciphertexts have a one-to-one mapping, which, as with ECB, allows observers to distinguish repeated messages.

I forgot to mention that. Thanks. (This may not matter for some applications.)

--  
Kristian Gjøsteen  
.