

## Re: AES trick...

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-07/msg00507.html>

---

- *From:* "Tom St Denis" <[tomstdenis@xxxxxxxxx](mailto:tomstdenis@xxxxxxxxx)>
  - *Date:* 15 Jul 2006 14:08:11 -0700
- 

Tom St Denis wrote:

The most common way to implement AES in 32/64 bit words is with the 8x32 tables and use register renaming for ShiftRows.

My trick I want to explore [and I'm seeing if anyone else tried this] is just to use a static 16-tuple of 8x128 tables [64KB] for the entire round function. Since ShiftRows and MixColumns are linear you could just implement the entire round function as 16 lookups and 15 xors.

Hmm, it'd be smarter to just byte access plaintext block which has been brought up here before. hehehe.

Nevermind.

Tom

.