

## Re: fixed block size

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-04/msg00808.html>

---

- *From:* "Joseph Ashwood" <[ashwood@xxxxxxx](mailto:ashwood@xxxxxxx)>
  - *Date:* Thu, 26 Apr 2007 21:09:31 -0700
- 

"Antony Clements" <[antony.clements@xxxxxxxxxxxxxxxx](mailto:antony.clements@xxxxxxxxxxxxxxxx)> wrote in message [news:4630682e\\$0\\$11540\\$afc38c87@xxxxxxxxxxxxxxxxxxxxxxxx](news:4630682e$0$11540$afc38c87@xxxxxxxxxxxxxxxxxxxxxxxx)

given my realisation, on top of every other weakness people have found in my layer, is a fixed block size in this instance yet another avenue of attack?

While I can see where the idea is coming from, and I can also see where mathematically there is an argument that having multiple block sizes can offer some extra protection, I do not see an advantage of a variable block size over using the largest block size of the system. The reasoning is fairly straight-forward, by using the variable block length you are in effect consuming key space for selecting that block size, by doing this you are limiting the possible {domain, range, key} combinations and leaking information about the key in every block boundary, by fixing the block length no information has to be leaked at the block boundary. A fairly straightforward example is to look at the Vigenere cipher, whose block length is the key length, this provides extra leverage on the key in that if the block length can be found the key length is immediately discovered.

The core problem comes down to providing leverage to the attacker, it should be fairly obvious that giving the attacker any leverage is a bad idea.

Joe

.