

Re: My little something...

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-08/msg00155.html>

- *From:* Peter Fairbrother <zenadsl6186@xxxxxxxxxx>
 - *Date:* Tue, 18 Jul 2006 18:24:45 +0100
-

Tom St Denis wrote:

Markus Jansson wrote:

And there is no reason to assume that the combo is more secure,

There is no reason to believe it is LESS secure. On the contrary, if two ciphers are cascaded and 1 of them fails, the second one still keeps the encryption secure. Why you cannot understand this?

Because the notion of "more secure" doesn't follow. You're defending against unknown attacks. The problem is unknown attacks are unknown [see below].

You are wrong to classify the threat (not the attack) as unknown, it is well-defined – that a TLA will break (or has broken) EAS.

The TLAs would dearly like to do that, and no doubt have spent some resources trying to do so. AES is the big target, the one that resources will be thrown at.

Does a break of AES imply a break of Twofish? No. Possibly, but by no means necessarily, a break for EAS might also apply to Twofish, but AES and Twofish are very different structurally.

There are algebraic relationships in AES that don't exist in Twofish and most other ciphers. An attack based on one of those relationships would almost certainly not affect Twofish or Serpent, and they look to be the most promising basis for an attack on AES – or say rather they look like they might be the weakest point in AES.

Re: My little something...

Using double encryption with two different ciphers of different structure defends against the threat of such a break in AES, and in many circumstances will cost nothing significant at all, just a few free cycles. In a typical PC application the user will never notice.

So you have the security of AES – and if someone breaks AES but not Serpent you do not become insecure. If this comes at no cost other than a few lines of code, surely that is not a misappropriation of resources.

[...]

and besides, since you are double crypting there is a MITM attack. So it's not a good idea.

MITM attack would only be possible if I used SAME CIPHER twice. Im not. Im using Twofish + Serpent for example.

That's not true unfortunately.

I assume he is still using a 128/256-bit security level, and not trying to increase the effective key size, so the meet-in-the-middle attack is neither threatening, relevant or interesting.

[...]

You assume your adversary is something like the NSA or a government because you have no idea what cryptography is actually for. You think it's all cloak and dagger. Which is cute and all, just totally naive.

I don't know the OP, so can't comment – but if your or my security system can defeat the attacks of NSA, that will mean almost every other form of attacker is defeated too, so why not use NSA as the threat model attacker?

I know I routinely do (but then my crypto is more likely than most to actually be attacked by NSA).

Do you think your crypto, eg libtomcrypt, would withstand an attack by NSA?

Yeah yeah, resources – but the OP mentioned that this was meant to be secure against TLAs, so bitching about that gets you nowhere.

Neither is explaining that most breaks come from side-channel attacks

Re: My little something...

Re: My little something...

germane to the question of whether using double encryption with different ciphers is useful or economic.

[...]

Enigma wasn't broken in the 30s. They knew how to attack it in the 40s but it still required a machine to do some of the manual labour.

Marian Rejewski first broke Enigma in 1932. There were later variants which were broken later.

[...]

Chances that BOTH AES and WHATEVER are broken are SMALLER than chances of just AES being broken. Why cant you get this?

Because it isn't true?

Oh yes it is.

Look at Differential or Linear cryptanalysis.
Suppose you used Snefru+Knufu as your ciphers. DC broke both of them.
It's entirely possible to chain an attack through both and recover the key. It's entirely possible that whatever attack renders AES completely insecure can also be used against other block ciphers.

Khufu?

Snefru? Isn't that a hash?

In any case, DC broke some ciphers and didn't break some others. The ones which broke were mostly similar in structure – many ciphers with different structures were not affected by DC. I wouldn't have suggested using two structurally similar ciphers together in double encryption for precisely that reason, as well as because there might be some unnoticed relationship between their permutations which might weaken security.

If I was to pick two ciphers for double encryption I would choose two that were as dissimilar as possible. If I had done that beforehand there is a very good chance that my system would have been unaffected by the discovery of DC – a much better chance than if I had only chosen one cipher. It would only have taken one resistant choice to maintain security.

Re: My little something...

Re: My little something...

No, but atleast Im a bit more prepared than you are, who have NO countermeasures at all. If AES is broken, you are screwed. If AES is broken, my AES+WHATEVER still remains secure. Why cant you get this?

Because it isn't true.

Not necessarily true, no – but it is possibly, and even probably, true.

And if it is true, and you didn't use both – well, that's a tradeoff. But if there is zero cost to a perhaps–much–better–and–certainly–no–worse encipherment and you don't use it, that's a bad tradeoff.

--

Peter Fairbrother

.