

Re: AES design – can you help me to understand

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-06/msg01456.html>

- *From:* "kentucky" <pam@xxxxxxxxxxxx>
 - *Date:* Fri, 30 Jun 2006 23:16:17 +0930
-

"Tom St Denis" <tomstdenis@xxxxxxxx> wrote in message
<news:1151673948.223453.59920@xx>

kentucky wrote:

Here we go:
DES uses a key dependant transformation in every round?

Um that's one way to put it I guess, we tend to look at the round function as constant with the input being permuted (e.g. XOR'ed with a key derived from the secret key through a key schedule)

AES uses a scrambling scheme that alternates between:
[1] The use of a transformation that does not interact with "additional" key material
[2] Followed by another scrambling operation that does interact with key dependant information.

Um? A "round" of AES is

subbyte
shiftrows
mixcolumns
addroundkey

Not sure but I think the paper was suggesting that

subbyte
shiftrows
mixcolumns

Re: AES design – can you help me to understand

May be a key independant scrambling round?

addroundkey

And this one may be a key dependant scrambling round similar to what DES uses in every round?

Together, "key-alternating" round strategy?

Every round of AES uses key material derived from the secret key through a key schedule.

Just for discussion, so I can understand:

If one ran DES and AES for an equal number of rounds – say 10:

DES outputs see an "image" of the key 10 times?

AES outputs see an "image" of the key material 5 times?

I have no idea what "sees an image" means. But it's wrong anyways. In 10 rounds of AES there are **11** round keys

Suggesting, (keeping all of the other complexities constant) that DES outputs have a higher probability of leaking information about the key into the outputs than AES does?

Um only if the round keys are highly correlated [which they are in DES and to a lesser extent AES]. If you learn 1 bit of a DES round key you learn 1 bit of the secret key. The same is not always [but might as well be I guess] true for AES.

I mean the key material is being used directly and more frequently in DES?

On a per round basis, no.

Let's say for argument only, that DES does leak a bit of information about the key into its outputs. Then, it seems to follow that AES should leak less key information, for the same number of rounds, into AES outputs, all other

Re: AES design – can you help me to understand

Re: AES design – can you help me to understand
factors being equal?

The AES key schedule is a shift register. If you learn one rounds
round key you're hosed.

PS.

It would be nice [for those deficient with the "notation"]
if someone could demo the ideas from section 3.4
with example data so that the operations specified
therein can be better understood and made concrete?

I'm writing a book on this. :-) Wait till October 2006.

Or ... Buy the Rijndael book. I imagine that explains the design in
great detail.

Failing that there are many other resources on the web that explain
AES. There are even wikipedia entries and of course John Savards
interesting diagrams :-)

Tom