

Re: counter mode and data integrity

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/3081.html>

From: flip (flip_alpha_at_safebunch.com)

Date: 10/31/03

Date: Fri, 31 Oct 2003 06:55:21 -0800

"Joerg Platte" <Joerg.Platte@uni-dortmund.de> wrote in message
news:bnt7fi\$7r\$1@nx6.HRZ.Uni-Dortmund.DE...

> *Hi!*

>

> *I want to encrypt a file using AES in counter mode to allow random access.*

> *To prevent reuse of the counter I can't use the block number as counter.*

> *Hence, I must store the counter value, and a SHA-1 hash to ensure data
> integrity, for every block with the file.*

>

> *But I don't want to store the counter value for every block to save some*

> *bytes. I'm thinking about to use the hash value (computed with the data*

> *concatenated with the block number) as counter. This ensures data*

integrity

> *and a different counter value for every block. If two blocks are the same*

> *the concatenated block number should prevent the same counter value.*

>

> *Where can I find some information about this "special" counter mode? Is it*

> *secure?*

>

> *regards,*

> *Joerg*

>

Have you seen the modes of operation put out by NIST? Perhaps google on Nist
+ CTR Mode?

Also, there are papers available for ctr mode from the authors (see the
NIST) web site.

HTH, Flip