Subject: Re: Protect package - A starting copy protection system
Posted by mdelfede on Sat, 25 Sep 2010 13:37:13 GMT
View Forum Message <> Reply to Message

Zbych wrote on Sat, 25 September 2010 13:36AES is quite small. See attached files that implement AES256 encryption. I use them on small 8-bit uC like AVR.

Hi Zbych,

thank you for the source
As I see, AES is a block-encoder with a blocksize of 128 bits and a keysize of 128, 192 or 256 bits, right ?
If so, I'll have to adapt it to my routines, as they need to encode/decode variable sized buffers.
Just one question : if I encode 2 128 bit blocks, let's say block 1 and block 2, and I want to decode them in reverse order, like block 2 and then block 1, shall I care about something, like resetting the encoder between blocks ?

Ciao

Max