Subject: Re: Protect package - A starting copy protection system
Posted by Zbych on Sat, 25 Sep 2010 16:03:28 GMT
View Forum Message <> Reply to Message

Those routines implement ECB (electronic codebook) mode. That means that every block of data is encoded separately. It is safer to use CBC mode with long data streams.

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

If you use ECB mode, you don't have to reset encoder, just initialize ctx at the begging. Since you want to encrypt blocks of code, you can tell compiler to align code to 16 bytes (in case of gcc you can add inline assembly with align directive).