

Re: Beginner Qn: Encrypting small data

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-06/2195.html>

From: Michael Amling (*nospam_at_nospam.com*)

Date: 06/30/04

Date: Wed, 30 Jun 2004 15:32:17 GMT

kackson wrote:

- > *Hi.*
- > *This is the first time I'm working to encrypt some data. So, any*
- > *advise or pointer to sites or books are deeply appreciated.*
- >
- > *I need to encrypt (and of course decrypt) data that is not larger*
- > *than 500KB in real time (i.e. less than one fifth or 0.2 of a sec).*
- > *Since the data is easily accessible by unauthorized users, I would*
- > *also need the method to easily render the entire data useless once a*
- > *single byte of information is altered. Are there existing algorithm or*
- > *some combination of methods that could achieve that? Or should I read*
- > *up more books and cook up my algorithm?*
- >
- > *Thanks in advance.*

You could try AES in CTR mode with an HMAC-SHA1. You need a good source of entropy for making up the random keys.

If this is just temporary data, stored on disk and then read back in by the program still running, then storing the keys should not be a problem. Otherwise, you need to think about how the legitimate user will get and supply the keys (passphrase, public key cryptography, etc).

—Mike Amling