

Re: PLEASE HELP – How do I include OpenSSL in my code? <OT: Cryptographic laws>

Re: PLEASE HELP – How do I include OpenSSL in my code? <OT: Cryptographic laws>

Source: http://coding.derkeiler.com/Archive/C_CPP/comp.lang.c/2006-05/msg02793.html

- *From:* "Malcolm" <regnizar@xxxxxxxxxxxxxxxx>
 - *Date:* Wed, 17 May 2006 23:29:01 +0100
-

"Richard Heathfield" <invalid@xxxxxxxxxxxxxxxx> wrote in message

True; of course, most people who hear that believe that ciphertext[i] = plaintext[i] ^ 5 is a "reasonably secure cryptosystem".

And so it is, provided nobody actually tries to crack it (which, again, is true of most cryptosystems!).

When people do try to roll their own, it is sometimes embarrassing to see just how quickly they can be broken. A guy I used to work with came up with what he thought was an uncrackably complex scheme. He had spent several days designing it. He gave me no algorithm, just some ciphertext, and it took me about ten minutes. <sigh>

But if you are scanning every email sent in the country, for the string "Mr Vladimir orders three quarts of cheese", then those ten minutes are prohibitive.

--

www.personal.leeds.ac.uk/~bgy1mm