

Re: ecb works , but cfb and cbc don't (php)

Re: ecb works , but cfb and cbc don't (php)

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-08/msg00502.html>

- *From:* Paul Rubin <<http://phr.cx@xxxxxxxxxxxxxxxx>>
 - *Date:* 22 Jul 2006 17:54:34 -0700
-

veg_all@xxxxxxxx writes:

actually all my encrypted files are plaintext , with everything in hexadecimal. I just convert the binary to hex and store it all in a simple file. i can then ftp, email this file anywhere and decrypt it as long as I know the key.

I think you should use an existing program like GnuPG/PGP to encrypt your files, instead of trying to write your own program. Getting this stuff right takes a considerable amount of knowledge.

.