

Re: Question on Symmetric encryptions algorithms:

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-06/1466.html>

From: Henrick Hellström (henrick.hellstrm_at_telia.com)

Date: 06/28/03

Date: Sat, 28 Jun 2003 00:11:18 GMT

Shashank Khanvilkar wrote:

- > *Is it possible that a symmetric encryption algorithm (aes-128-cbc, say) can*
- > *actually produce an encrypted output file which is smaller in size than the*
- > *original input file.*
- > *Will appreciate any help.*

No, that is not possible, but:

- 1) it is not unusual that crypto software compress the input before encryption, and
- 2) primitives such as AES might be used for other purposes than encryption, e.g. for message authentication (AES-CBC-MAC) or hashing (e.g. the DES-based unix password hash) and the output of such constructs is usually the size of a single block.