Subject: Re: Encrypted storage with streaming (OpenSSL, AES)
Posted by koldo on Mon, 22 Feb 2010 06:54:00 GMT
View Forum Message <> Reply to Message

Hello Mindtraveller

Quote:1) Key must be 128/192/256 bits long. User password may have ANY length.
2) Key is very important part of cryptographic strength of overall encryption. Using criptographically weak key (user password in 99,9% of cases is extremely weak) turns all AES encryption into weak and rather breakable system. As well as using cryptographically strong key makes overall AESStream system extremely unbreakable to anyone.

Does it mean that AES cannot be used for saving user files with user defined password ?

However there are programs that include this possibility with AES. For example 7zip offers AES-256 encryption http://www.7-zip.org/7z.html.

Is there a standard way to convert a 8 chars user defined password into an useful 256 AES bits key ?