Subject: Re: Encrypted storage with streaming (OpenSSL, AES)
Posted by Mindtraveller on Sun, 21 Feb 2010 23:48:53 GMT
View Forum Message <> Reply to Message

Hello, Koldo.

I have found bug in AESStream which led to different original and decoded strings in the example. Also I got rid of Web/SSL dependency. Just tested it, and everything seems fine.

Please try updated version of AESStream and read it's tutorial if you want to use it in your app. Tutorial say that you should not use user password instead of generated key.

Why?
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.

File Attachments

1) AESStream.zip, downloaded 516 times