Subject: Re: StreamCypher - A package for stream data cryptography
Posted by Mindtraveller on Sat, 02 Oct 2010 06:15:15 GMT
View Forum Message <> Reply to Message

Quote:If also the state machines are different, I'd vote for 2 classes. I don't really know exactly how it works in OpenSSL implementation. I just use it. And the ways, I use it for decryption/encryption in my classes, are different. Again: these are two different state machines in my case, that is why I'd prefer 2 classes instead of one.

Quote:No, I think we have to keep just the S-Boxes in memory, which is far safer OK. I have to add s-box support into AES classes too.

Quote:Well, both Cypher and Crypto are equally good Then I'd suggest Crypto as it sounds closer to Decrypt/Encrypt classes.

Please let me know when you make common interface for our classes.