Subject: Re: StreamCypher - A package for stream data cryptography
Posted by mdelfede on Fri, 01 Oct 2010 15:50:51 GMT
View Forum Message <> Reply to Message

Hi Honza,

did you try with the reference implementation of Snow2.0 instead of the fast version ? It should be easier to port, and anyways we don't need a very fast encryption for PHP side, we just need to encrypt some small strings.

About the package, I'll implement first the interface, then add the already coded RC4 and Snow2, then we could add some other encryptors.

I've got to add some stuffs to Protect too.... the initialization vectors, for example, they're still missing.
Then I'd like to take your PHP and add a web auth module to Protect.... even with just plain RC4 if you couldn't port Snow to PHP. We can add the rest later

Ciao

Max