Subject: Cypher package - An extensible Encryption package
Posted by mdelfede on Sat, 02 Oct 2010 23:42:41 GMT
View Forum Message <> Reply to Message

I uploaded the very first implementation of a generic encryption package, as discussed in topic

http://www.ultimatepp.org/forum/index.php?t=msg&th=5568& amp; amp; amp;start=0&

I tried to have an interface as modular as possible in order to be able to merge all current Encryption packages.

It has a base class defining the interface; supports String, Block and Streaming encryption.
By now it implements RC4 and Snow2 Streaming symmetric encryptors.

Other modules should derive from CypherBase class and implement ALL of its pure virtual functions in order to keep the interface identical.

Package still miss error handling, it'll implemented when we'll agree on the interface proposed.
Docs are missing too, for the same reason.

There's also an extensible testing application, which allow to select the encryption module, the encryption mode and some more.

Pavel, could you look if the interface meets your needs too ?
It still miss the Initialization Vector handling, I've got some ideas on how to make it fit yours and my needs, but before implementing it I'd like the interface to be stable enough.

Ciao

Max

EDIT : Please wait to review package... I'm making still many changes in interface and moving most routines to base class.

Max