Subject: Re: Cypher package - An extensible Encryption package
Posted by mdelfede on Sun, 03 Oct 2010 18:38:46 GMT
View Forum Message <> Reply to Message

Interface should be stable enough, also the streaming part is working.

There are 2 functions to define in derived classes :

```
// main encoding/decoding function
// must be redefined on each derived class
virtual void Cypher(byte const *sourceBuf,  byte *destBuf, size_t bufLen) = 0;

// main key setting function
// must be redefined on each derived class
virtual bool CypherKey(byte const *keyBuf, size_t keyLen, byte const *nonce, size_t
nonceLen) = 0;
```

Plus, you must give BlockSize in constructor in case of Block Cyphers like AES.

Streaming is done with << operator (stream in) and >> operator (stream out).
For block cyphers, there's a Flush() function which pads last block with random data and returns size of encoded stream (true size, without padding). When decoding, using SetStreamSize(size) allows the decoder to un-pad the last block and return cleaned stream.

Block mode is fully supported, with checking of block size in case of Block-Cyphers.
Encoding/Decoding in block mode is done by some overloaded operator() which supports String encoding and binary buffer encoding, in place and out of place.

The test app CypherTest now supports both test with block and streaming modes.

Still missing a couple of small stuffs, but it should be stable enough now.

Ciao

Max