Subject: Re: StreamCypher - A package for stream data cryptography
Posted by Mindtraveller on Thu, 30 Sep 2010 20:01:15 GMT
View Forum Message <> Reply to Message

I fully support idea of making uniform interface.
We may even have one parent virtual class like CryptoEncoder and make our implementations as it's descendants. This could be useful for flexibility of usage in user code.

Let's discuss interface in detail.

1. Constructors
Snow2() - OK
Snow2(const String &key) - OK
Snow2(byte const *keyBuf, int keyLen) - I believe first parameter should be const byte *keyBuf (in your case you define pointer which points to changeable data but cannot be changed itself).

2. Same for SetKey.
BTW, what do you do if user tries to encrypt with no key set?

3. Agreed with Encode interface with exception as in (1) with change (byte const *) to (const byte *).

4. My encoder works with data of any size. It just internally adds random data for stream to be of 128-bit (not byte!) aligned size.