Subject: Re: StreamCypher - A package for stream data cryptography
Posted by mdelfede on Thu, 30 Sep 2010 12:49:47 GMT
View Forum Message <> Reply to Message

Yep, that could be done.
We should indeed change some of both codes to have an uniform interface.
I have those :

```
	// constructors
	Snow2();
	Snow2(const String &key);
	Snow2(byte const *keyBuf, int keyLen);

	// key settings
	bool SetKey(const String &key);
	bool SetKey(byte const *keyBuf, int keyLen);

	// encode string
	String Encode(String const &s);

	// encode buffer, dest on different buffer
	void Encode(byte const *sBuf, byte *dBuf, dword bufLen);

	// encode buffer in place
	void Encode(byte *buf, dword bufLen);
```

(this for Snow2, exactly the same for RC4 encoding)

So I shall add streaming capabilities as your code, with operators << and >>; you should add the same as I have in my code above, so we'll have an uniform interface.
Is it feasible for you ?
For me, I could add dynamic streaming capabilities, as I've no need of a fixed block size.

Ah, BTW... AFAIK AES works on blocks of fixed size of 128 bits.... is the same for your encoder ?
I mean... you must work on multiple of 128 bytes ?

Ciao

Max