Subject: Re: StreamCypher - A package for stream data cryptography
Posted by dolik.rce on Fri, 01 Oct 2010 16:31:56 GMT
View Forum Message <> Reply to Message

mdelfede wrote on Fri, 01 October 2010 17:50Hi 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.
Well, the trouble is not really the complexity. The biggest problem is the low level approach. Both the slow and the fast reference implementations use type dependent tricks, which makes it nightmare in php as it has only one integer type which has no idea about signedness and to make it even more fun it's range is platform dependent. I managed to rewrite it into working php code, it "just" doesn't work correctly I guess I missed some of the overflows. It might be actually easier to implement it from scratch looking only in specs... But I'll definitely keep trying, it drives me mad when I can't achieve something so simple (~400 lines of code)

Honza