

Re: Another SHA2 implementation

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-05/0060.html>

From: Juuso Hukkanen (juuso929_at_tele3d.net)

Date: 05/02/05

Date: Mon, 02 May 2005 01:21:37 +0300

On 1 May 2005 13:19:19 -0700, "Tom St Denis" <tomstdenis@gmail.com> wrote:

>*Juuso Hukkanen wrote:*

>> *Thank You Tom :D*

>> *I admit, You are the person I have mostly tried to persuade here. I*

>> *will mail You some details next weekend. This project is huge, but it*

>> *has a small, but significant chance to success.*

>

>*What project? Rewriting LibTom in a new language that nobody uses?*

Don't worry, only a list of opensource software projects that I like to include to GPL stule ChOS license. I have said earlier that language will be released on mid-juni. Because it contains stuff which could be easily patented or spoiled, I will not share special info about anything with anyone before the release. On release day you all may flame me – if you don't like the t3d. Basically it is now as ready as it will be in 1.5 months – now it rests as documents.

Language is massive – compare with PHP, so it is nobodys 'task' to write big portions of it. I publish it some code parts and advertice it around the net maybe some functions and libraries will drop then from heaven. Importantly the language does not need a critical code mass to work, it is ready to use immediately after release.

Only thing to do before t3d release is the license that is legal-part-ChOS and including suggested projects (many of which will never be done). But if some then good – even exellent. Why ChOS license and those included Projects? A: When t3d started to look like a superiour language, I concluded it to be so good it could carry some ballast. Well that GPL-style license is a ballast(and also a possibility), but think the language is really that good – Good enough to have people writing with it useful programs for larger audience... ultimately collecting money to charity from rich country companies.

So the license is the only problem, I must have that before releasing the language. And that license must be written openly with some help from *.legal newsgroups.However they can not help with suggested projects list, other than being terrified. That is why I need coding/crypto expertise and was thinking about You as a project

description (in)sanity checker. I dont want to describe projects which are not possible and then see license carring impossible projects for years. And that only because I newer asked a second opinion or asked for suggestions better than my thoughts. Damn hey, I can post them here and have non-crypto related stuff <OT> marked. Ok, everybody will be able to express their thoughts and flames here.

Yes I will do that, there will be possible many opinions lots of flaming and even JSH will likely think that I've lost my touch with reality. But who cares. At least it will be different topics. Unfortunately this is the only possible way to achieve goals – by thinking Big Big Big. It sure would be great to be able to release the thing with GPL, and then next day say that lets include the charity organization aspect...and day after could also a certain project idea...

Later much later with the language, I was hoping something like if You could check that the language parts which use LibTomCrypt use it correctly – because I guess nobody else knows its performance as well. Obviously Crypto functions are definately not the first ones the language needs – but they will be in it heart. (For example I'd like that all network communication would start with a PKI-Hello and exchange of communication keys – >all network communication with t3d would be encrypted as default) . Is that heavy default-encryption worth including? It would be exellent to know that at least in theory your LibTomCrypt expert knowledge could sometimes be available – Not to cause you stress or annoyance. Noooo. The language is good, trust me, you are going to like it allready on 2005/06/15 :)

Juuso Hukkanen