Haskell Cryptographic Library 4.2.0

Dominic Steinitz

December 23, 2013

The Haskell Cryptographic Library 4.2.0[1] collects together existing Haskell cryptographic functions into one cabalized package, together with HUnit tests, QuickCheck property tests and examples. It is a significant change from previous versions and now only contains cryptographic functions; the functions for dealing with ASN.1, X.509 certificates and PKCS#8 will be provided by an entirely separate library reducing the number of dependencies.

This release contains:

- DES
- Blowfish
- AES
- TEA
- Cipher Block Chaining (CBC)
- PKCS#5 and nulls padding
- SHA-1
- MD5
- RSA

Haddock documentation for the library is available here[2] .

1 System Requirements

- The code has been tested on GHC 6.6 and Hugs Version September 2006. It does not currently work with YHC because of the lack of `Data.Word` and `Data.Bits`.
- It *no longer* requires the use of `NewBinary.Binary`.

[1] http://www.haskell.org/crypto
[2] http://www.haskell.org/crypto/doc/html

2 Installation Instructions

Get the sources:

```
darcs get --tag "4.2.0" http://code.haskell.org/crypto
```

Build and install ready for testing:

```
ghc -o Setup Setup.hs -package Cabal
./Setup configure --prefix=/my/chosen/dir
./Setup build
./Setup install --user
```

Run the tests.

```
cd /my/chosen/dir/bin
./RSATest
./SymmetricTest
./QuickTest
```

You can now run the examples to confirm further that everything is working satisfactorily. When you are happy, build and install them in their final destination:

```
./Setup unregister --user
./Setup clean
./Setup configure
./Setup build
./Setup install
```

3 To Do

In no particular order:

- Incorporate other symmetric key algorithms already coded in Haskell.
- Performance analysis as Blowfish ought to run more quickly than DES.
- Other modes / padding schemes.
- Extend typechecking to ensure that only the appropriate key sizes are used for a given algorithm.
- Improve performance, for example, for SHA1. This code[3] runs an order of magnitude faster but, with respect to the authors, doesn't feel that functional.
- Get rid of the GPL code.

4 Contact

All questions, comments, bug reports, flames, requests for updates / changes and suggestions should be directed to Dominic Steinitz and logged here[4] .

[3] http://www.abridgegame.org/repos/darcs-unstable
[4] http://hackage.haskell.org/trac/crypto

5 Licensing

The modules in the library come from different authors and have been released under different licences.

5.1 Contributors

5.1.1 Codec.Binary

Codec.Binary.BubbleBabble	John Meacham	Copyright © 2008, All rights reserved	BSD

5.1.2 Codec.Text

Codec.Text.Raw	Dominic Steinitz	Copyright © 2006, All rights reserved	BSD

5.1.3 Codec.Encryption

Codec.Encryption.AES	Lukasz Anforowicz	Copyright © 2005, All rights reserved	BSD
Codec.Encryption.AESAux	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD
Codec.Encryption.Blowfish	Doug Hoyte	Copyright © 2005, All rights reserved	BSD
Codec.Encryption.BlowfishAux	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD
Codec.Encryption.TEA	John Meacham	Copyright © 2008, All rights reserved	BSD
Codec.Encryption.DES	Ian Lynagh	Copyright © 2005, All rights reserved	BSD
Codec.Encryption.DESAux	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD
Codec.Encryption.Modes	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD
Codec.Encryption.Padding	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD
Codec.Encryption.RSA	David Sankel	Copyright © 2005, All rights reserved	GPL
Codec.Encryption.RSA.EMEOAEP	David Sankel	Copyright © 2005, All rights reserved	GPL
Codec.Encryption.RSA.MGF	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD
Codec.Encryption.RSA.NumberTheory	David Sankel	Copyright © 2005, All rights reserved	GPL

5.1.4 Codec

Codec.Utils	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD

5.1.5 Data.Digest

Data.Digest.MD5	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD
Data.Digest.MD5Aux	Ian Lynagh	Copyright © 2005, All rights reserved	BSD
Data.Digest.SHA1	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD

5.1.6 Data

Data.LargeWord	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD

5.1.7 Tests and Examples

RSATest	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD
QuickTest	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD
SymmetricTest	Dominic Steinitz	Copyright © 2005, All rights reserved	BSD

5.2 The BSD License

This license is based on The BSD License[5].

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT ONWERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[5] http://www.opensource.org/licenses/bsd-license.php

5.3 The GNU General Public License (GPL)

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You can find a copy of the GNU General Public License here[6] ; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

6 Disclaimer

Cryptography is a notoriously easy area in which to make mistakes, not necessarily with the algorithms but with how they are implemented (for example not protecting keys, using weak keys and so on). For a readable account of some of the pitfalls, see Ross Anderson[7] 's book.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT ONWERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

7 Acknowledgements

- Doug Hoyte (HardCore SoftWare)
- Anatoly Zaretsky
- Ian Lynagh[8]
- David Sankel[9]
- Ross Paterson[10]
- Lukasz Anforowicz
- Warrick Gray[11]

[6] http://www.opensource.org/licenses/gpl-license.php
[7] http://www.cl.cam.ac.uk/users/rja14/
[8] http://web.comlab.ox.ac.uk/oucl/work/ian.lynagh
[9] http://www.electronconsulting.com/whois.html
[10] http://www.soi.city.ac.uk/ ross
[11] http://homepages.paradise.net.nz/warrickg/haskell/http/

- Russell O'Connor[12]
- Spencer Janssen

[12] http://r6.ca