GEYKE93
Librerías adicionales

Algunos algoritmos y funciones de las siguientes librerías fueron incorporados en GEYKE93. La instalación de dichas se puede realizar directamente desde esta carpeta o a través de las respectivas direcciones oficiales (en el caso de otras versiones). Se detalla a continuación la versión utilizada y los contenidos.

1 Crypto++

Fue hecha por Wei Dai en 1995 y soporta sistemas de 34 y 64 bits para muchos sistemas operativos dentro de los que se encuentra Android (usando STLport), Apple (MAC OS X e iOS), BSD, Linux, Solaris y Windows. Compiladores de esta librería: MSVC 2012, GCC 4.7, Clang 3.2, Solaris Studio 12.3, Intel C++ Compiler 13.0.

Versión 5.6.2. (February 20, 2013) Detalles de esta versión:

- Se incorpora SHA-3 (Keccak)
- Previa licencia de Crypto++ cambia por Boost Software License 1.0 http://www.boost.org/ que es un set de librerías de $C++$
- Entre otros.

http://www.cryptopp.com/

Después de extraer el .zip presente en esta carpeta o la dirección electrónica señalada, revisar el README.txt.

Sobre la licencia: The License of Crypto++ is somewhat unusual amongst open source projects. A distinction is made between the library as a compilation (i.e., collection), which is copyrighted by Wei Dai, and the individual files in it, which are public domain. The library is copyrighted as a compilation in order to place certain disclaimers (regarding warranty, export, and patents) in the license and to keep the attributions and public domain declarations intact when Crypto++ is distributed in source code form. The fact that individual files are public domain means that legally you can place code segments, entire files, or small sets of files (up to the limit set by fair use) into your own project and do anything you want with them without worrying about the copyright.

Esta librería incluye: ciphers, message authentication codes, one-way hash functions, public-key cryptosystems, and key agreement schemes.

2 Beecrypt

BeeCrypt es un proyecto que provee un amplio, rápido y fuerte kit de criptografía que puede ser utilizado en gran variedad de aplicaciones debido a que no está diseñado para resolver un único problema como otras librerías. Contiene C altamente optimizado e implementaciones de algoritmos como Blowfish, MD5, SHA-1, Diffie-Hellman, and ElGamal. Incluye entropy sources, random generators, block ciphers, hash functions, message authentication codes, multiprecision integer routines, and public key primitives.

Esta librería es software libre que puede ser redistribuida y/o modificada bajo los térmios de GNU Lesser General Public License. Ver Free Software Foundation.

La version revisada fue 4.1.2 (estable del 21 diciembre 2004).

La instalación y documentación se puede acceder a través de las siguientes direcciones o el file dentro de esta carpeta.

http://packages.debian.org/source/wheezy/beecrypt
http://beecrypt.sourceforge.net/
http://sourceforge.net/projects/beecrypt/

http://beecrypt.sourceforge.net/doxygen/c/

Esta librería puede ser accesada desde Java bajo la instalación de BeeCrypt for Java. Ha sido probada para las siguientes plataformas:

1. Cygwin
2. Darwin/MacOS X
3. Linux glibc 2.x alpha
4. Linux glibc 2.x arm
5. Linux glibc 2.x ia64
6. Linux glibc 2.x m68k
7. Linux glibc 2.x ppc
8. Linux glibc 2.x s390
9. Linux glibc 2.x s390x
10. Linux glibc 2.x sparc
11. Linux glibc 2.x x86
12. Tru64 Unix alpha
13. Win32 (Windows 95, 98, NT 4.0, 2000, XP)

3 hashlib++

Se revisó la versión 0.3.4. (13 octubre 2011)

hashlib++ es una librería simple y fácil utilizada para crear una checksum crptográfica (llamado hash function) a través de un único method-call que debería funcionar en cualquier compilador o plataforma. Su licencia es de BSD-license, osea que es software libre.

Documentación en Doxygen
http://hashlib2plus.sourceforge.net/doc/sourcedoc/index.html
Revisar README.tex

Extraer el .zip indicado.