This package was debianized by Ivo Timmermans <ivo@debian.org> on

Fri, 3 Aug 2001 10:02:38 +0200.

It was taken over by Matthias Urlichs <smurf@debian.org>, and is now

maintained by Andreas Metzler <ametzler@debian.org> Eric Dorland

<eric@debian.org>, James Westby <jw+debian@jameswestby.net>

It was downloaded from https://ftp.gnupg.org/gcrypt/libgcrypt/.

Up to end of 2012 libgcrypt copyright was owned solely by FSF, since then

contributions without copyright assignment to the FSF have been integrated.

Upstream Authors (from AUTHORS)

8X---------------------------------------------------

List of Copyright holders

=========================

Copyright (C) 1989,1991-2019 Free Software Foundation, Inc.

Copyright (C) 1994 X Consortium

Copyright (C) 1996 L. Peter Deutsch

Copyright (C) 1997 Werner Koch

Copyright (C) 1998 The Internet Society

Copyright (C) 1996-1999 Peter Gutmann, Paul Kendall, and Chris Wedgwood

Copyright (C) 1996-2006 Peter Gutmann, Matt Thomlinson and Blake Coverett

Copyright (C) 2003 Nikos Mavroyanopoulos

Copyright (C) 2006-2007 NTT (Nippon Telegraph and Telephone Corporation)

Copyright (C) 2012-2019 g10 Code GmbH

Copyright (C) 2012 Simon Josefsson, Niels MÃ¶ller

Copyright (c) 2012 Intel Corporation

Copyright (C) 2013 Christian Grothoff

Copyright (C) 2013-2017 Jussi Kivilinna

Copyright (C) 2013-2014 Dmitry Eremin-Solenikov

Copyright (C) 2014 Stephan Mueller

Copyright (C) 2017 Bundesamt fÃ¼r Sicherheit in der Informationstechnik

Authors with a FSF copyright assignment

=======================================

LIBGCRYPT Werner Koch 2001-06-07

Assigns past and future changes.

Assignment for future changes terminated on 2012-12-04.

wk@gnupg.org

Designed and implemented Libgcrypt.

GNUPG Matthew Skala 1998-08-10

Disclaims changes.

mskala@ansuz.sooke.bc.ca

Wrote cipher/twofish.c.

GNUPG Natural Resources Canada 1998-08-11

Disclaims changes by Matthew Skala.

GNUPG Michael Roth Germany 1998-09-17

Assigns changes.

mroth@nessie.de

Wrote cipher/des.c.

Changes and bug fixes all over the place.

GNUPG Niklas Hernaeus 1998-09-18

Disclaims changes.

nh@df.lth.se

Weak key patches.

GNUPG RÃ©mi Guyomarch 1999-05-25

Assigns past and future changes. (g10/compress.c, g10/encr-data.c,

g10/free-packet.c, g10/mdfilter.c, g10/plaintext.c, util/iobuf.c)

rguyom@mail.dotcom.fr

ANY g10 Code GmbH 2001-06-07

Assignment for future changes terminated on 2012-12-04.

Code marked with ChangeLog entries of g10 Code employees.

LIBGCRYPT Timo Schulz 2001-08-31

Assigns past and future changes.

twoaday@freakmail.de

LIBGCRYPT Simon Josefsson 2002-10-25

Assigns past and future changes to FSF (cipher/{md4,crc}.c, CTR mode,

CTS/MAC flags, self test improvements)

simon@josefsson.org

LIBGCRYPT Moritz Schulte 2003-04-17

Assigns past and future changes.

moritz@g10code.com

GNUTLS Nikolaos Mavrogiannopoulos 2003-11-22

nmav@gnutls.org

Original code for cipher/rfc2268.c.

LIBGCRYPT The Written Word 2005-04-15

Assigns past and future changes. (new: src/libgcrypt.pc.in,

src/Makefile.am, src/secmem.c, mpi/hppa1.1/mpih-mul3.S,

mpi/hppa1.1/udiv-qrnnd.S, mpi/hppa1.1/mpih-mul2.S,

mpi/hppa1.1/mpih-mul1.S, mpi/Makefile.am, tests/prime.c,

tests/register.c, tests/ac.c, tests/basic.c, tests/tsexp.c,

tests/keygen.c, tests/pubkey.c, configure.ac, acinclude.m4)

LIBGCRYPT Brad Hards 2006-02-09

Assigns Past and Future Changes

bradh@frogmouth.net

(Added OFB mode. Changed cipher/cipher.c, test/basic.c doc/gcrypt.tex.

added SHA-224, changed cipher/sha256.c, added HMAC tests.)

LIBGCRYPT Hye-Shik Chang 2006-09-07

Assigns Past and Future Changes

perky@freebsd.org

(SEED cipher)

LIBGCRYPT Werner Dittmann 2009-05-20

Assigns Past and Future Changes

werner.dittmann@t-online.de

(mpi/amd64, tests/mpitests.c)

GNUPG David Shaw

Assigns past and future changes.

dshaw@jabberwocky.com

(cipher/camellia-glue.c and related stuff)

LIBGCRYPT Andrey Jivsov 2010-12-09

Assigns Past and Future Changes

openpgp@brainhub.org

(cipher/ecc.c and related files)

LIBGCRYPT Ulrich MÃ¼ller 2012-02-15

Assigns Past and Future Changes

ulm@gentoo.org

(Changes to cipher/idea.c and related files)

LIBGCRYPT Vladimir Serbinenko 2012-04-26

Assigns Past and Future Changes

phcoder@gmail.com

(cipher/serpent.c)

Authors with a DCO

==================

Andrei Scherer <andsch@inbox.com>

2014-08-22:BF7CEF794F9.000003F0andsch@inbox.com:

Christian Aistleitner <christian@quelltextlich.at>

2013-02-26:20130226110144.GA12678@quelltextlich.at:

Christian Grothoff <christian@grothoff.org>

2013-03-21:514B5D8A.6040705@grothoff.org:

Dmitry Eremin-Solenikov <dbaryshkov@gmail.com>

2013-07-13:20130713144407.GA27334@fangorn.rup.mentorg.com:

Dmitry Kasatkin <dmitry.kasatkin@intel.com>

2012-12-14:50CAE2DB.80302@intel.com:

JÃ©rÃ©mie CourrÃ¨ges-Anglas <jca@wxcvbn.org>

2016-05-26:87bn3ssqg0.fsf@ritchie.wxcvbn.org

Jussi Kivilinna <jussi.kivilinna@mbnet.fi>

2012-11-15:20121115172331.150537dzb5i6jmy8@www.dalek.fi:

Jussi Kivilinna <jussi.kivilinna@iki.fi>

2013-05-06:5186720A.4090101@iki.fi:

Markus Teich <markus dot teich at stusta dot mhn dot de>

2014-10-08:20141008180509.GA2770@trolle:

Mathias L. Baumann <mathias.baumann at sociomantic.com>

2017-01-30:07c06d79-0828-b564-d604-fd16c7c86ebe@sociomantic.com:

Milan Broz <gmazyland@gmail.com>

2014-01-13:52D44CC6.4050707@gmail.com:

Peter Wu <peter@lekensteyn.nl>

2015-07-22:20150722191325.GA8113@al:

RafaÃ«l CarrÃ© <funman@videolan.org>

2012-04-20:4F91988B.1080502@videolan.org:

Sergey V. <sftp.mtuci@gmail.com>

2013-11-07:2066221.5IYa7Yq760@darkstar:

Stephan Mueller <smueller@chronox.de>

2014-08-22:2008899.25OeoelVVA@myon.chronox.de:

TomÃ¡Å¡ MrÃ¡z <tm@t8m.info>

2012-04-16:1334571250.5056.52.camel@vespa.frost.loc:

Vitezslav Cizek <vcizek@suse.com>

2015-11-05:20151105131424.GA32700@kolac.suse.cz

Werner Koch <wk@gnupg.org> (g10 Code GmbH)

2012-12-05:87obi8u4h2.fsf@vigenere.g10code.de:

More credits

============

Libgcrypt used to be part of GnuPG but has been taken out into its own

package on 2000-12-21.

Most of the stuff in mpi has been taken from an old GMP library

version by Torbjorn Granlund <tege@noisy.tmg.se>.

The files cipher/rndunix.c and cipher/rndw32.c are based on those

files from Cryptlib. Copyright Peter Gutmann, Paul Kendall, and Chris

Wedgwood 1996-1999.

The ECC code cipher/ecc.c was based on code by Sergi Blanch i Torne,

sergi at calcurco dot org.

The implementation of the Camellia cipher has been taken from the

original NTT provided GPL source.

The CAVS testing program tests/cavs\_driver.pl is not to be considered

a part of libgcrypt proper. We distribute it merely for convenience.

It has a permissive license and is copyrighted by atsec information

security corporation. See the file for details.

The file salsa20.c is based on D.J. Bernstein's public domain code and

taken from Nettle. Copyright 2012 Simon Josefsson and Niels MÃ¶ller.

This file is free software; as a special exception the author gives

unlimited permission to copy and/or distribute it, with or without

modifications, as long as this notice is preserved.

This file is distributed in the hope that it will be useful, but

WITHOUT ANY WARRANTY, to the extent permitted by law; without even the

implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

8X---------------------------------------------------

License:

Most of the package is licensed under the GNU Lesser General Public

License (LGPL) version 2.1 (or later), except for helper and debugging

binaries. See below for details. The documentation is licensed under

the GPLv2 (or later), see below.

Excerpt from upstream's README:

The library is distributed under the terms of the GNU Lesser

General Public License (LGPL); see the file COPYING.LIB for the

actual terms. The helper programs (e.g. gcryptrnd and getrandom)

as well as the documentation are distributed under the terms of

the GNU General Public License (GPL); see the file COPYING for the

actual terms.

This library used to be available under the GPL - this was changed

with version 1.1.7 with the rationale that there are now many free

crypto libraries available and many of them come with capabilities

similar to Libcrypt. We decided that to foster the use of

cryptography in Free Software an LGPLed library would make more

sense because it avoids problems due to license incompatibilities

between some Free Software licenses and the GPL.

Please note that in many cases it is better for a library to be

licensed under the GPL, so that it provides an advantage for free

software projects. The Lesser GPL is so named because it does

less to protect the freedom of the users of the code that it

covers. See http://www.gnu.org/philosophy/why-not-lgpl.html for

more explanation.

An example of the license headers of the LGPL is

-------------

Copyright (C) 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2006

2007, 2008, 2009, 2010, 2011 Free Software Foundation, Inc.

This file is part of Libgcrypt.

Libgcrypt is free software; you can redistribute it and/or modify

it under the terms of the GNU Lesser General Public License as

published by the Free Software Foundation; either version 2.1 of

the License, or (at your option) any later version.

Libgcrypt 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 Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public

License along with this program; if not, see <http://www.gnu.org/licenses/>.

-------------

On Debian GNU/Linux systems, the complete text of the GNU Lesser

General Public License can be found in

`/usr/share/common-licenses/LGPL';

The documentation licensed under the GPL

-------------

Copyright @copyright{} 2000, 2002, 2003, 2004, 2006, 2007, 2008, 2009, 2011, 2012 Free Software Foundation, Inc. @\*

Copyright @copyright{} 2012, 2013, 2016 2017 g10 Code GmbH

@quotation

Permission is granted to copy, distribute and/or modify this document

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. The text of the license can be found in the

section entitled ``GNU General Public License''.

-------------

Further details on licensing:

From upstream's LICENSES file

8X---------------------------------------------------

Additional license notices for Libgcrypt. -\*- org -\*-

This file contains the copying permission notices for various files in

the Libgcrypt distribution which are not covered by the GNU Lesser

General Public License (LGPL) or the GNU General Public License (GPL).

These notices all require that a copy of the notice be included

in the accompanying documentation and be distributed with binary

distributions of the code, so be sure to include this file along

with any binary distributions derived from the GNU C Library.

\* BSD\_3Clause

For files:

- cipher/sha256-avx-amd64.S

- cipher/sha256-avx2-bmi2-amd64.S

- cipher/sha256-ssse3-amd64.S

- cipher/sha512-avx-amd64.S

- cipher/sha512-avx2-bmi2-amd64.S

- cipher/sha512-ssse3-amd64.S

#+begin\_quote

Copyright (c) 2012, Intel Corporation

All rights reserved.

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.

\* Neither the name of the Intel Corporation nor the names of its

contributors may be used to endorse or promote products derived from

this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY INTEL CORPORATION "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 INTEL CORPORATION 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.

#+end\_quote

For files:

- random/jitterentropy-base.c

- random/jitterentropy.h

- random/rndjent.c (plus common Libgcrypt copyright holders)

#+begin\_quote

\* Copyright Stephan Mueller <smueller@chronox.de>, 2013

\*

\* License

\* =======

\*

\* Redistribution and use in source and binary forms, with or without

\* modification, are permitted provided that the following conditions

\* are met:

\* 1. Redistributions of source code must retain the above copyright

\* notice, and the entire permission notice in its entirety,

\* including the disclaimer of warranties.

\* 2. 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.

\* 3. The name of the author may not be used to endorse or promote

\* products derived from this software without specific prior

\* written permission.

\*

\* ALTERNATIVELY, this product may be distributed under the terms of

\* the GNU General Public License, in which case the provisions of the GPL are

\* required INSTEAD OF the above restrictions. (This clause is

\* necessary due to a potential bad interaction between the GPL and

\* the restrictions contained in a BSD-style copyright.)

\*

\* THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED

\* WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES

\* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF

\* WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR 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 NOT ADVISED OF THE POSSIBILITY OF SUCH

\* DAMAGE.

#+end\_quote

\* X License

For files:

- install.sh

#+begin\_quote

Copyright (C) 1994 X Consortium

Permission is hereby granted, free of charge, to any person obtaining a copy

of this software and associated documentation files (the "Software"), to

deal in the Software without restriction, including without limitation the

rights to use, copy, modify, merge, publish, distribute, sublicense, and/or

sell copies of the Software, and to permit persons to whom the Software is

furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in

all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE

X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN

AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNEC-

TION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the X Consortium shall not

be used in advertising or otherwise to promote the sale, use or other deal-

ings in this Software without prior written authorization from the X Consor-

tium.

#+end\_quote

\* Public domain

For files:

- cipher/arcfour-amd64.S

#+begin\_quote

Author: Marc Bevand <bevand\_m (at) epita.fr>

Licence: I hereby disclaim the copyright on this code and place it

in the public domain.

#+end\_quote

\* OCB license 1

For files:

- cipher/cipher-ocb.c

#+begin\_quote

OCB is covered by several patents but may be used freely by most

software. See http://web.cs.ucdavis.edu/~rogaway/ocb/license.htm .

In particular license 1 is suitable for Libgcrypt: See

http://web.cs.ucdavis.edu/~rogaway/ocb/license1.pdf for the full

license document; it basically says:

License 1 â€” License for Open-Source Software Implementations of OCB

(Jan 9, 2013)

Under this license, you are authorized to make, use, and

distribute open-source software implementations of OCB. This

license terminates for you if you sue someone over their

open-source software implementation of OCB claiming that you have

a patent covering their implementation.

License for Open Source Software Implementations of OCB

January 9, 2013

1 Definitions

1.1 â€œLicensorâ€ means Phillip Rogaway.

1.2 â€œLicensed Patentsâ€ means any patent that claims priority to United

States Patent Application No. 09/918,615 entitled â€œMethod and Apparatus

for Facilitating Efficient Authenticated Encryption,â€ and any utility,

divisional, provisional, continuation, continuations-in-part, reexamination,

reissue, or foreign counterpart patents that may issue with respect to the

aforesaid patent application. This includes, but is not limited to, United

States Patent No. 7,046,802; United States Patent No. 7,200,227; United

States Patent No. 7,949,129; United States Patent No. 8,321,675 ; and any

patent that issues out of United States Patent Application No. 13/669,114.

1.3 â€œUseâ€ means any practice of any invention claimed in the Licensed Patents.

1.4 â€œSoftware Implementationâ€ means any practice of any invention

claimed in the Licensed Patents that takes the form of software executing on

a user-programmable, general-purpose computer or that takes the form of a

computer-readable medium storing such software. Software Implementation does

not include, for example, application-specific integrated circuits (ASICs),

field-programmable gate arrays (FPGAs), embedded systems, or IP cores.

1.5 â€œOpen Source Softwareâ€ means software whose source code is published

and made available for inspection and use by anyone because either (a) the

source code is subject to a license that permits recipients to copy, modify,

and distribute the source code without payment of fees or royalties, or

(b) the source code is in the public domain, including code released for

public use through a CC0 waiver. All licenses certified by the Open Source

Initiative at opensource.org as of January 9, 2013 and all Creative Commons

licenses identified on the creativecommons.org website as of January 9,

2013, including the Public License Fallback of the CC0 waiver, satisfy these

requirements for the purposes of this license.

1.6 â€œOpen Source Software Implementationâ€ means a Software

Implementation in which the software implicating the Licensed Patents is

Open Source Software. Open Source Software Implementation does not include

any Software Implementation in which the software implicating the Licensed

Patents is combined, so as to form a larger program, with software that is

not Open Source Software.

2 License Grant

2.1 License. Subject to your compliance with the term s of this license,

including the restriction set forth in Section 2.2, Licensor hereby

grants to you a perpetual, worldwide, non-exclusive, non-transferable,

non-sublicenseable, no-charge, royalty-free, irrevocable license to practice

any invention claimed in the Licensed Patents in any Open Source Software

Implementation.

2.2 Restriction. If you or your affiliates institute patent litigation

(including, but not limited to, a cross-claim or counterclaim in a lawsuit)

against any entity alleging that any Use authorized by this license

infringes another patent, then any rights granted to you under this license

automatically terminate as of the date such litigation is filed.

3 Disclaimer

YOUR USE OF THE LICENSED PATENTS IS AT YOUR OWN RISK AND UNLESS REQUIRED

BY APPLICABLE LAW, LICENSOR MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY

KIND CONCERNING THE LICENSED PATENTS OR ANY PRODUCT EMBODYING ANY LICENSED

PATENT, EXPRESS OR IMPLIED, STATUT ORY OR OTHERWISE, INCLUDING, WITHOUT

LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR

PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL LICENSOR BE LIABLE FOR ANY

CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE,

ARISING FROM OR RELATED TO ANY USE OF THE LICENSED PATENTS, INCLUDING,

WITHOUT LIMITATION, DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE

OR SPECIAL DAMAGES, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF

SUCH DAMAGES PRIOR TO SUCH AN OCCURRENCE.

#+end\_quote

8X---------------------------------------------------

On Debian GNU/Linux systems, the text of the GNU General Public License,

version 2 can be found in `/usr/share/common-licenses/GPL-2'.