

Copyright and licensing of the Python Cryptography Toolkit ("PyCrypto"):

Previously, the copyright and/or licensing status of the Python Cryptography Toolkit ("PyCrypto") had been somewhat ambiguous. The original intention of Andrew M. Kuchling and other contributors has been to dedicate PyCrypto to the public domain, but that intention was not necessarily made clear in the original disclaimer (see [LEGAL/copy/LICENSE.orig](#)).

Additionally, some files within PyCrypto had specified their own licenses that differed from the PyCrypto license itself. For example, the original RIPEMD.c module simply had a copyright statement and warranty disclaimer, without clearly specifying any license terms. (An updated version on the author's website came with a license that contained a GPL-incompatible advertising clause.)

To rectify this situation for PyCrypto 2.1, the following steps have been taken:

1. Obtaining explicit permission from the original contributors to dedicate their contributions to the public domain if they have not already done so. (See the "LEGAL/copy/stmts" directory for contributors' statements.)
2. Replacing some modules with clearly-licensed code from other sources (e.g. the DES and DES3 modules were replaced with new ones based on Tom St. Denis's public-domain LibTomCrypt library.)
3. Replacing some modules with code written from scratch (e.g. the RIPEMD and Blowfish modules were re-implemented from their respective algorithm specifications without reference to the old implementations).
4. Removing some modules altogether without replacing them.

To the best of our knowledge, with the exceptions noted below or within the files themselves, the files that constitute PyCrypto are in the public domain. Most are distributed with the following notice:

The contents of this file are dedicated to the public domain. To the extent that dedication to the public domain is not available, everyone is granted a worldwide, perpetual, royalty-free, non-exclusive license to exercise all rights associated with the contents of this file for any purpose whatsoever.
No rights are reserved.

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 AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Exceptions:

- Portions of HMAC.py and setup.py are derived from Python 2.2, and are therefore Copyright (c) 2001, 2002, 2003 Python Software Foundation (All Rights Reserved). They are licensed by the PSF under the terms of the Python 2.2 license. (See the file [LEGAL/copy/LICENSE.python-2.2](#) for details.)
- The various GNU autotools (autoconf, automake, aclocal, etc.) are used during the build process. This includes macros from autoconf-archive, which are located in the m4/ directory. As is customary, some files from the GNU autotools are included in the source tree (in the root directory, and in the build-aux/

directory). These files are merely part of the build process, and are not included in binary builds of the software.

EXPORT RESTRICTIONS:

Note that the export or re-export of cryptographic software and/or source code may be subject to regulation in your jurisdiction.