

## GnuPG 2.0 - IDEA support

#####  
The article was obtained at the following URL: <http://www.kfwebs.net/articles/article/42>  
The article might be distributed further as long as it is provided as it is, with the credits stated.  
The Article was written and first published by KF Webs, at <http://www.kfwebs.net>  
#####

*Added: 2006-11-15 17:08:57 - Modified: 2007-06-23 12:02:31 - Level: Advanced*

## International Data Encryption Algorithm

IDEA is short for International Data Encryption Algorithm. The cipher was designed under a research contract with the Hasler Foundation, which became part of Ascom-Tech AG. The cipher is patented in a number of countries but is freely available for non-commercial use. The name "IDEA" is also a trademark. The patents will expire in 2010 - 2011. Today, IDEA is licensed worldwide by MediaCrypt.

IDEA was used in Pretty Good Privacy (PGP) V2.0, and was incorporated after the original cipher used in v1.0 ("Bass-O-Matic") was found to be insecure. It is an optional algorithm in OpenPGP.

IDEA is patented in at least Austria, France, Germany, Italy, Japan, The Netherlands, Spain, Sweden, Switzerland, The UK and The US.

## What is this?

This is a package to add IDEA support to GnuPG 2.0 / libgrypt in order to be backwards compatible with e.g PGP 2.0

I threw this together in a couple of hours one evening when I was bored, so it is bound to have some errors in it, but I got to decrypt the emails I wanted to, so I'm happy with it. If you find any obvious oddity, however, don't hesitate to [contact me](#)

## Installation

The .tar.bz2 file contains three files, the idea.c file that is to be placed in libgrypt's cipher directory and the gcrypt.diff that contains some instructions on a couple of files to alter. Run a ./configure on the libgrypt package, apply the necessary changes, and do a make && sudo make install && sudo ldconfig, and it should show up when doing gpg2 --version as: Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH

The file gnupg.diff is to be executed as "patch < gnupg.diff" from within the GnuPG 2.0.x g10 directory, that is, this file is not related to libgrypt.



**Updated: 2007-06-23:**

Alon Bar-Lev has cleaned up the patch some and merged it all into a single diff file that can be [downloaded here](#) [[sig](#)]. GnuPG also needs [this patch](#) [[sig](#)] by Alon. It might be easier to get working than the original version. Gentoo users should be able to emerge libgcrypt with the idea USE-flag

## Old files

Download [gcrypt.tar.bz2](#) [[OpenPGP Signature](#)]

## Credits

The idea.c file is based on the idea.c file used for gnupg version 1., which again is based on an implementation from Bruce Schneier: Applied Cryptography. John Wiley & Sons, 1996. ISBN 0-471-11709-9.

## Related articles:

[PHP Sendmail classes](http://www.kfwebs.net/articles/article/15)[<http://www.kfwebs.net/articles/article/15>] ([PHP](#))