-----BEGIN PGP SIGNED MESSAGE-----

Enclosed is version 1.6 of FatMacPGP 2.6.3. This is a Macintosh port of the international version PGP 2.6.3ia released 04.03.96. The underlying PGP cryptographic code is the same as in the international release, except that it uses the RSAREF1.0 RSA library instead of Philip Zimmermann's MPILIB, in order to conform with US Patents on RSA. Also the legal_kludge switch, which allows interoperability with infringing pre-2.6 versions of PGP, is disabled.

FatMacPGP 2.6.3 will run in native mode on a Power Macintosh, and will also run on 68K Macintoshes having a 68020 CPU or better. It will NOT run on Macintoshes with only a 68000 CPU such as Pluses, SE's, Classics or PB100's.

It contains all the enhancements and bug fixes of PGP 2.6.3ia such as

1) It allows recipients of a public key message to be read in from a file containing the list of recipients, one per line. (Unlike previous versions of MacPGP it will not crash if the number of recipients exceeds 5 or 7.)
2) When extracting multiple keys into an ascii file, the each key is put separately into its own block, neatly labelled with the key id and user ids.
3) Better support for 8 bit character sets, ie. characters you get by holding down the option key.
4) Userids can be automatically signed with your secret key when creating keys ('pgp -kg') or adding new userids ('pgp -ke'). This is controlled by the AutoSign flag in the Options menu.
5) The misfeature of the initial 2.6.3i release, which didn't allow softwrapped text to be treated as text has been removed.
6) When clearsigning messages, FatMacPGP 2.6.3 will add a "Charset:" headerto the signature block, explaining which character set was used for creating the signature. This will help the recipient of the message to select correct character conversion when verifying the signature. If he/she is using version 2.6.3i, PGP will automatically choose the correct character set, thereby eliminating a lot of "Bad signature" problems.

In addition to the above FatMacPGP 2.6.3 has many enhancements and bug fixes relative to previous versions of MacPGP.

1) Unlike MIT MacPGP 2.6.2 contains native Power PC code. Consequently it runs typically about 1.5 to 2 times faster than the MIT version on PPC machines, and even faster for large keyrings or large keys. It also runs typically 10-20% faster on 68K machines.
2) It has a greatly enhanced AppleEvent suite. For instance, unlike the MIT version, it is not necessary to write data to temporary files before passing it to MacPGP for en/de/cryption or signing. FatMacPGP 2.6.3 accepts AppleEvent TEXT parameters up to 32K in size in memory and returns the processed data as a parameter to the reply AppleEvent. (See the accompanying documentation for further details.)
3) It has options for automatic hardwrapping and detabbing of text, which should make electronic transmission of clearsigned messages more reliable and increase interoperability with many DOS and Unix text processing programs.
4) It has an option for stealthifying PGP encrypted files, removing any trace of their provenance. The resulting files can't be distinguished from white noise and can be completely concealed by "stegoing" into graphics and audio files. (There is of course also an option for destealthifying.)
5) It has an option for using SHA1 as the hashing algorithm for PGP signatures, instead of MD5. (Dobbertin has recently made some dramatic progress towards cryptanalyzing MD5. If he is successful, this might call into question the reliability of PGP signatures under certain circumstances.) This is an experimental feature which is not compatible with earlier versions of PGP. (It is not compatible with the proposed standards of PGP 3.0 either. But 3.0 is supposed to be deliberately incompatible with all 2.x versions to avoid the RSA patent issue.)

FatMacPGP 2.6.3 is distributed under the same license terms from MIT and RSADSI as the 2.6.2 release, since its functional core is virtually identical. Please read the license agreements prior to using the program. Distribution of this program may be subject to US government

export controls.

This release is not endorsed by Philip Zimmermann, MIT or anyone else.
However full source code for FatMacPGP 2.6.3 is being released together
with the executable (although in a separate archive). It is not difficult
to verify that the cryptographic core is unchanged from the 2.6.2 version.
Also the author is mentioned in Zimmermann's documentation as the
primary developer of previous MacPGP versions.

A few support files, such as sample AppleScripts and other extensions,
to facilitate interaction with the Eudora mailer program and the BBEdit
text editor are included. While they are fully functional and hopefully
useful, they are primarily intended to serve as illustrations to other
developers on how to integrate PGP with other Macintosh programs.
Detailed documentation can be found in the document "MacPGP263_AppleEvents"
in the Macintosh Documentation folder.

Read the included document "Verifying PGP" for instructions on how to
verify this copy of MacPGP. Beginners should first take a look at the
document "Getting Started with MacPGP". A detailed reference manual to
MacPGP entitled "MacPGP263_Manual" is enclosed in the Macintosh
Documentation folder and the indispensible "PGP User's Guide" by
Philip Zimmermann is in the Documentation folder.

Sources for FatMacPGP 2.6.3 are being distributed separately.

Z. Fiedorowicz

-----BEGIN PGP SIGNATURE-----
Version: 2.6.3
Charset: mac
Comment: MacPGP 2.6.3

iQCVAwUBMdVsvb1LYmqiC9QjAQFU3QP+IzAk5dZokGpcZ7myj8LmpafTsMf2NetK
dVnVq48rfTqU41bCKAQCrPYc8kM4Doe8TnE5WOO3IYol1+eMXSDOncafayk5JQx+
pFsi8lS+btF8MQLV40wutS+8du+8tYHlPGC4s2fsZL1CTWteS5ElBrILVL/YS2uH
sIgPRQjZV2c=
=bZJT
-----END PGP SIGNATURE-----