Pretty Good Privacy version 2.0 - READ ME FIRST

You are looking at the README file for PGP release 2.0. PGP, short for Pretty Good Privacy, is a public key encryption package; with it, you can secure messages you transmit against unauthorized reading and digitally sign them so that people receiving them can be sure they come from you.

The files pgpdoc1.txt and pgpdoc2.txt contain documentation for the system.

Before using PGP, PLEASE READ THE DOCUMENTATION. This tends to get neglected with most computer software, but cryptography software is easy to misuse, and if you don't use it properly much of the security you could gain by using it will be lost! You might also be unfamiliar with the concepts behind public key cryptography; the manual explains these ideas. Even if you are already familiar with public key cryptography, it is important that you understand the various security issues associated with using PGP.

The file SETUP.DOC contains information on how to install PGP on your system; this document is broken up into several sections, each dealing with a different operating system: PGP is known to run on MS-DOS, UNIX, and VMS. Part of the information in SETUP.DOC might make more sense if you have already read the manuals.

PGP 2.0, which was released on September 3, 1992, will likely be followed by updated versions within a few months of the release date. Bugs will likely be found and fixed, this being a new major release of the software, and we will try to get these fixes out to the public as soon as possible.

Given this, if you have received PGP 2.0 substantially after the initial release date, you may want to check around for a more recent release. If there is a more recent release, please acquire it, and please get the place you got PGP 2.0 from to update their release, too.

MANIFEST for PGP 2.0 MSDOS executable release

Here is a list of files included in the PGP 2.0 MSDOS executable release file PGP20.ZIP...

README.DOC	This file you are reading
SETUP.DOC	Installation guide
PGP.EXE	PGP executable program
CONFIG.TXT	User configuration parameter file for PGP
LANGUAGE.TXT	Sample language file for French and Spanish
PGP.HLP	Online help file for PGP
ES.HLP	Online help file in Spanish
FR.HLP	Online help file in French
PGPDOC1.DOC	PGP User's Guide, Vol I: Essential Topics
PGPDOC2.DOC	PGP User's Guide, Vol II: Special Topics
KEYS.ASC	Sample public keys to add to your keyring
PGPSIG.ASC	Detached signature of PGP.EXE, to detect viruses

For Clinical Paranoia Sufferers Only

It is always possible that the PGP you have received has been tampered with in some way. This is a risk because PGP is used as a system to assure security, so those wishing to breach your security could likely do it by making sure that your copy of PGP has been tampered with. Of course, if you receive PGP in a binary distribution, it makes sense to check it for viruses, and if you receive PGP as source code, looking for signs of obvious tampering might be a good idea. However, it is very difficult to actually determine if the code has no subtle bugs that have been introduced and that the executable you are using has not been tampered with in any way. If you are a really paranoid person, try getting a cryptographically signed copy of the software from someone you trust to have a good copy. It would also likely be good for you to read the sections of the manual on "Vulnerabilities", which you should have read anyway since you have read the documentation already, haven't you?