

PGP/GnuPG

Contributed by Mike Lyman
Saturday, 08 April 2006
Last Updated Thursday, 20 July 2006

What is PGP/GnuPG?

PGP is an encryption program that most people use with email. It uses very strong, public key cryptography to make messages unreadable except for the person who suppose to read it. It can also provide cryptographic, digital signatures so that a person can tell that the message came from the person it seems to have come from. GnuPG is an open source version that is free.

Why use PGP or GnuPG?

The same reason you don't write all your letters on postcards. When you send an email to somebody across the Internet, any computer system that touches it can make a copy of it and allow somebody to intercept the message and read it. By using PGP, only the person you want to see the message will see the message. It's like sending a letter in a locked envelope.

I've been a PGP user ever since I worked at AEGIS Research Corporation and one of our customers asked me to get him PGP and make it easy to use. Back then PGP was command line driven and not very easy for most people to use so we created a Windows front-end known as the AEGIS Shell that made PGP much easier to use. (Neither AEGIS nor I are supporting the AEGIS shell any more since there are Windows versions of PGP available these days.)

Recently I have mostly switched over to the GnuPG version of the program but still use the commercial version of PGP. If you are a Windows user, one of the best packages of GnuPG tools to use I have found is GPG4Win.

My Keys

If you wish to send me encrypted email or verify my PGP digital signatures, you will need my PGP keys.

Current Key: DH/DSS (DSA/ELG) (keyid: 0B7CE0828)
Expired Key: Diffie-Hellman/DSS key (keyid: 0xAB7F35DA)
Old Key: Diffie-Hellman/DSS key (keyid: 0xD7BBADAD)
Old Key: RSA key (keyid: 0x9441800D)
Original (revoked) Key RSA (keyid: 0xC34BEF45)