

Re: Beginner Question:Gnupg Decryption

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-03/msg00762.html>

- *From:* Peter Pearson <ppearson@xxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 26 Mar 2007 16:51:35 GMT
-

On 25 Mar 2007 22:14:02 -0700, MichiMichi <wwwmike@xxxxxx> wrote:

When I encrypt an email message with gnupg for multiple email recipients and then decrypt it again, I was under the assumption that I would need to specify both, the private keys passphrase and the key-id in order to decrypt

In the binary file produced by a gnupg encryption, I see 32-bit fields matching the four low-order bytes of the fingerprints of the public keys used for encryption. It seems reasonable to suppose that when undertaking to decrypt a message, gnupg extracts from the message a list of fingerprints of keys used in encrypting, and compares with a list of fingerprints for which the user knows the decryption keys, from the "secret" keyring.

When gnupg asks for the password to unlock the private key, you'll notice that it doesn't just ask for just any password; it asks for the password to use in unlocking a specific key, identified by fingerprint. Presumably this key was identified as the intersection of the two lists mentioned above.

--

To email me, substitute nowhere->spamcop, invalid->net.

.