Pretty Good Privacy – How to do it.

Tony Brett

IT Systems Manager
Corpus Christi College

OxCERT

Tel. (2)76695
tony.brett@ccc.ox.ac.uk

OUCS ITSS lunchtime seminar Tuesday 29th February 2000

What is PGP?

- Pretty Good Privacy
- 1976 – Diffie/Hellman
- 1977 – Rivest/Shamir/Adleman
- 1991 – Zimmermann writes PGP
- Send E-mail securely to a known recipient
- Digitally sign E-mail so that the recipient(s) can be sure it is from you
- Can also be used with file transfers

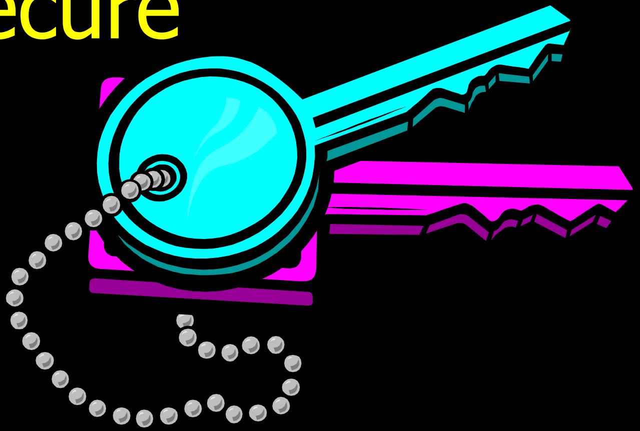
Why Bother?

- Sending plain text E-mail is little more secure than sending a postcard – PGP enables encryption
- PGP is useful for digitally signing material that is important (case of tutorials being cancelled)
- Enables secure transactions

  over E-mail.
- Pretty much unbreakable

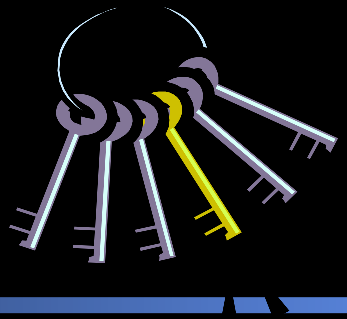
Key Pairs – public vs. private

- Types of Key – RSA vs DH/DSS
- Public is widely disseminated - private kept secret, with passphrase
- Fingerprints
- Varying levels of security. 512-bit lowest. 2048-bit very secure
- DEMO



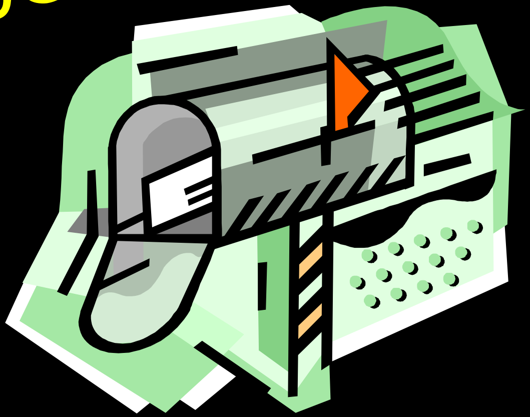
PGP Servers

- Servers that hold huge public key key rings
- Update to each other, accept and send updates from/to everyone
- Better than everyone keeping a huge key ring
- Server addresses included with PGP software



Encrypting messages

- Recipient’s public key is used to encrypt message
- Can use several different recipients’ public keys then any one of the matching private keys are required to decrypt message
- DEMO



Signing Messages

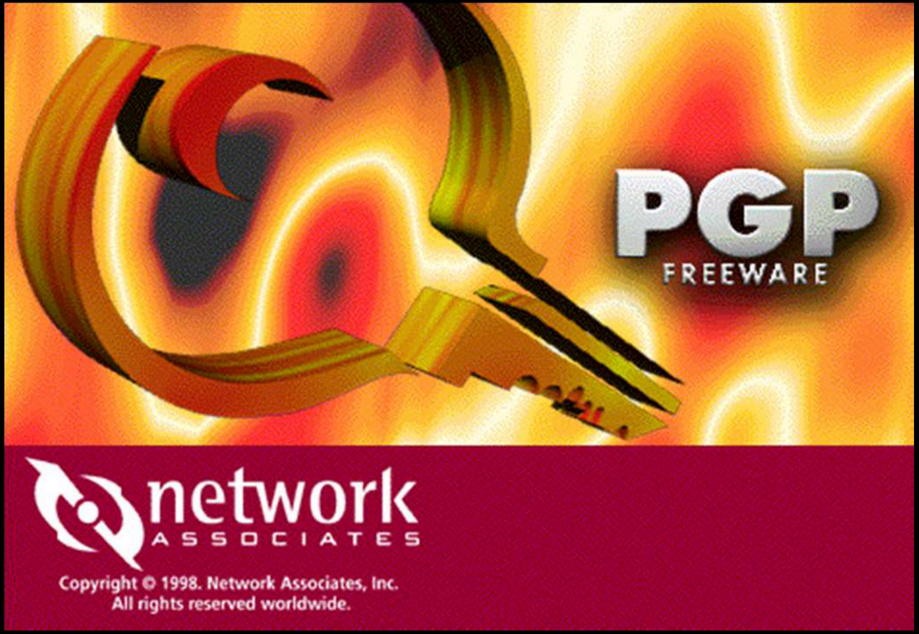
- Sender’s private key is used to encrypt some or all of the message
- Public key of sender is widely available so verification of signature is easy for anyone
- DEMO

Signing Keys. Why?

- How do you know that a person’s key is really theirs?
- Get owner to repeat fingerprint to you in person on on phone if you know their voice before signing key
- Unsigned keys are a security risk
- Key signing sessions involve just this
- http://www.ox.compsoc.net/compsoc/events/pgp-keysigning.html

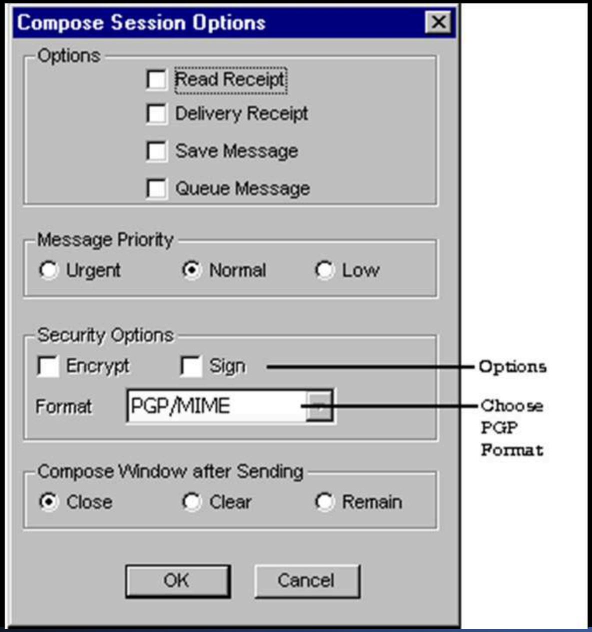
The Software

- Versions for PC, Mac, UNIX etc…
- Command-line & GUI
- ftp://ftp.ox.ac.uk/pub/pgp/pgpi/
- Version 6.0.2i
- Linewrap
- Sable/Ermine
- DEMO


PGP
FREEWARE
network
ASSOCIATES
Copyright © 1998. Network Associates, Inc.
All rights reserved worldwide.

Using PGP with Simeon (ExecMail)

- Plugin available for use with ExecMail 5.11 and PGP 6
- execmailsecurity-pgp6plug-in_130.exe
- DEMO



Compose Session Options

Options

□ Read Receipt
□ Delivery Receipt
□ Save Message
□ Queue Message

Message Priority

○ Urgent ● Normal ○ Low

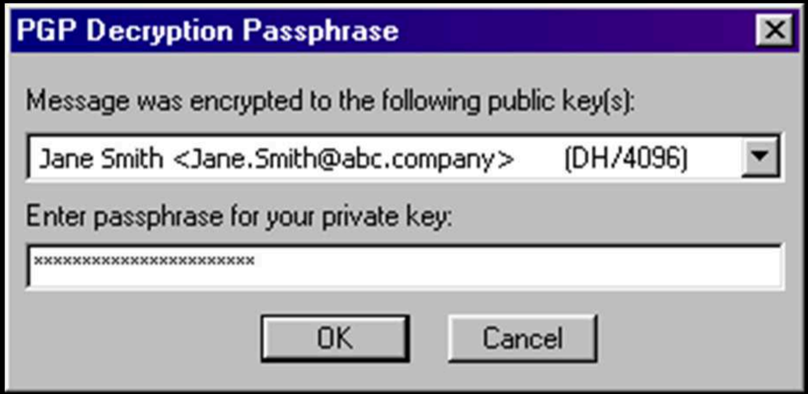
Security Options

□ Encrypt □ Sign

Format: PGP/MIME

Compose Window after Sending

● Close ○ Clear ○ Remain



PGP Decryption Passphrase

Message was encrypted to the following public key(s):

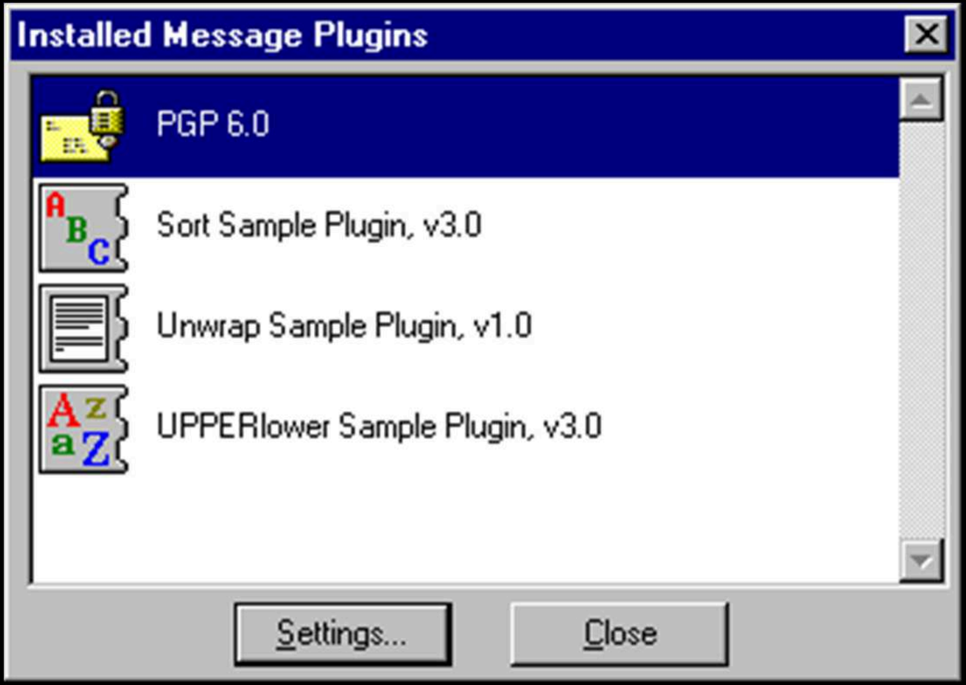
Jane Smith <Jane.Smith@abc.company> (DH/4096)

Enter passphrase for your private key:

****

Using PGP with Eudora, Outlook

- Plugins available with PGP 6.0.2i and above on Win32 at install time


Installed Message Plugins

PGP 6.0

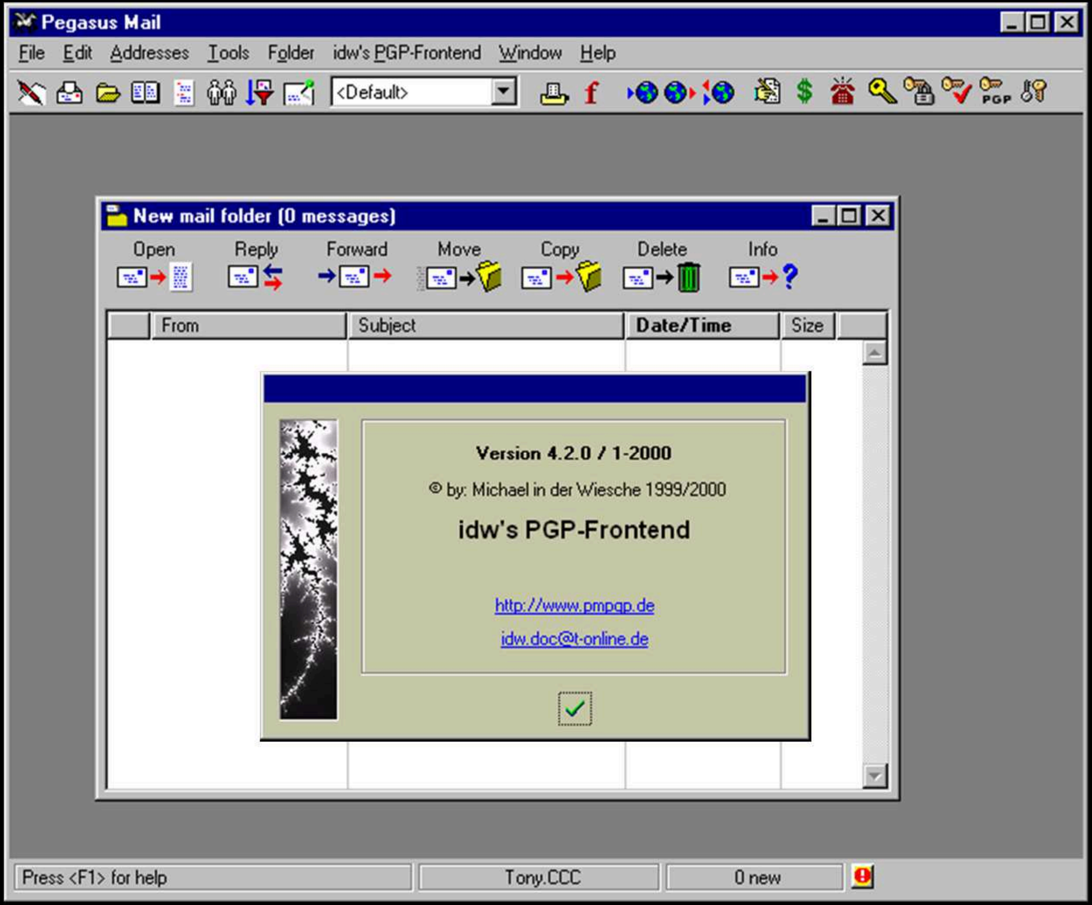
Sort Sample Plugin, v3.0

Unwrap Sample Plugin, v1.0

UPPERlower Sample Plugin, v3.0

Using PGP with Pegasus Mail

- http://www.pegasus.usa.com/encrypt.asp
- PGPMP



Version 4.2.0 / 1-2000

© by: Michael in der Wiesche 1999/2000

idw's PGP-Frontend

http://www.pmpgp.de

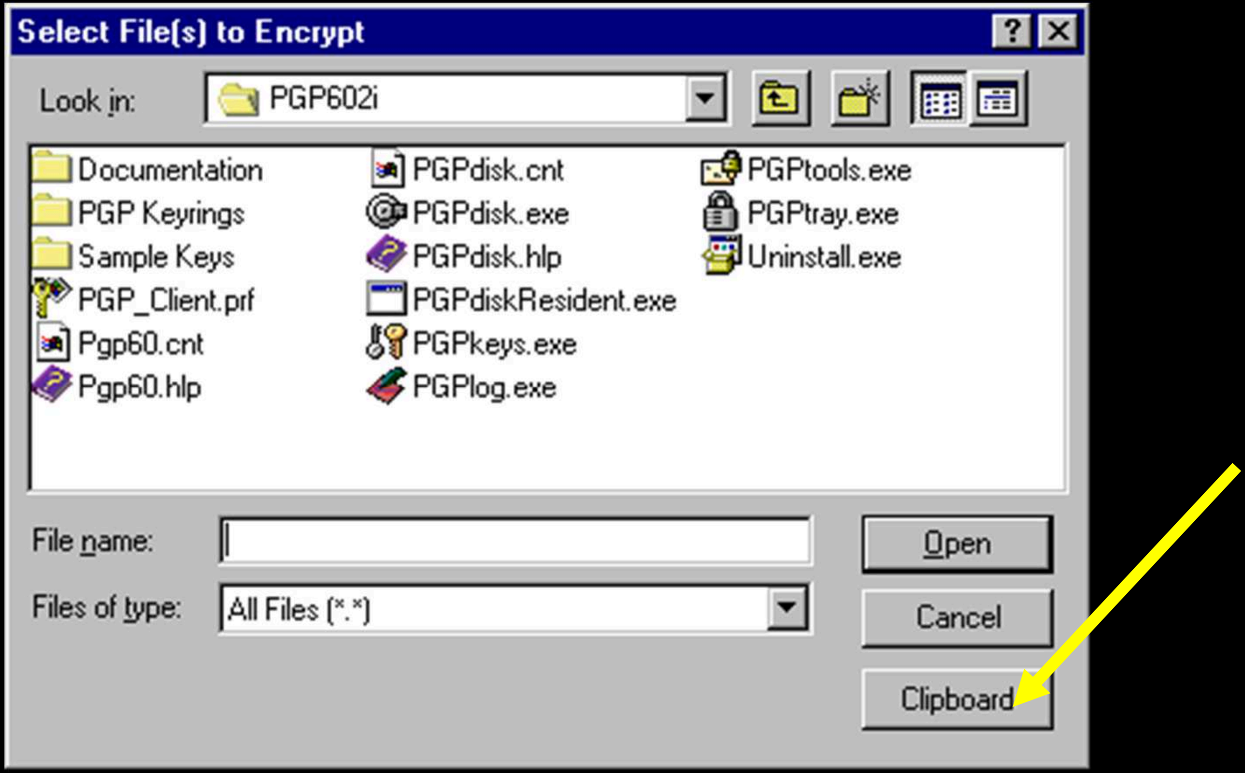
idw.doc@t-online.de

Using PGP with pine and elm on UNIX

- Mkpgp can be used with PINE
  - http://www.wsu.edu/UNIX_Systems/pgp/PGP-mkPGP-readme.html
- Elm has better in-built support than pine
- Can just extract files and manually decrypt or manually encrypt and include files

Using PGP with Herald (WING)

- Easiest here to use PGPs ability to encrypt/decrypt the clipboard
- DEMO



Select File(s) to Encrypt

Look in: PGP602i

Documentation
PGP Keyrings
Sample Keys
PGP_Client.prf
Pgp60.cnt
Pgp60.hlp
PGPdisk.cnt
PGPdisk.exe
PGPdisk.hlp
PGPdiskResident.exe
PGPkeys.exe
PGPlog.exe
PGPtools.exe
PGPtray.exe
Uninstall.exe

File name:

Files of type: All Files (*.*)

Resources

- http://www.oucs.ox.ac.uk/email/secure.html
- http://www.pgpi.org/
- http://www.pgpi.org/doc/faq/
- http://users.ox.ac.uk/~aesb/pgp.ppt

Questions

- This talk at: http://users.ox.ac.uk/~aesb/pgp.ppt