PGP (Pretty Good Privacy)

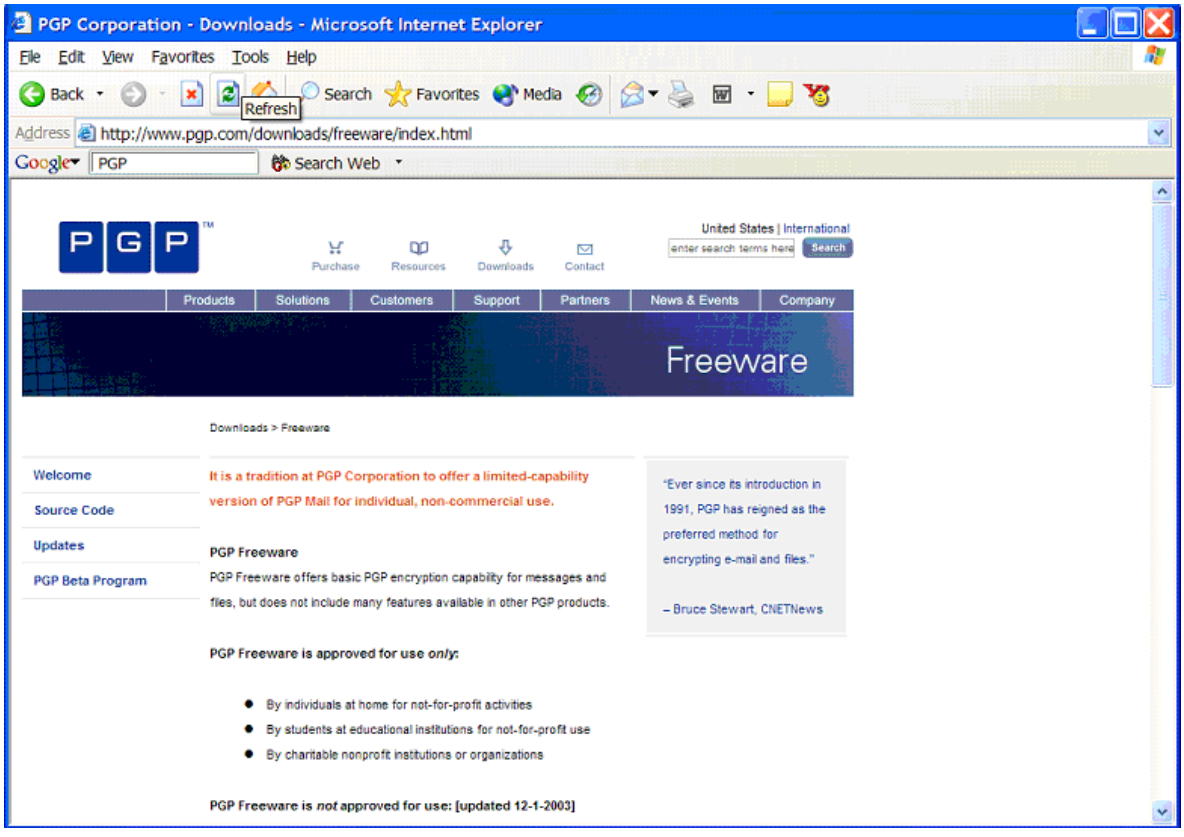
- *Pretty Good Privacy* atau *PGP* dikembangkan oleh Phil Zimmermann pada akhir tahu 1980. Pada mulanya, *PGP* digunakan untuk melindungi surat elektronik (*e-mail*) dengan memberi perlindungan kerahasiaan (enkripsi) dan otentikasi (tanda-tangan digital). Saat ini *PGP* tidak hanya ditujukan untuk keamanan *e-mail*, tetapi juga untuk keamanan berbagai file dan program pada komputer personal (*PC*).

- *PGP* menggunakan kriptografi simetri dan kriptografi kunci-publik. Oleh karena itu, *PGP* mempunyai dua tingkatan kunci, yaitu kunci rahasia (simetri) – yang disebut juga *session key* – untuk enkripsi data, dan pasangan kunci privat- kunci publik untuk pemberian tanda tangan dan melindungi kunci simetri.

- *PGP* tersedia sebagai *freeware* maupun sebagai paket komersil dalam berbagai versi yang dapat dioperasikan dalam berbagai sistem operasi (*DOS*, *Windows*, *UNIX*, *Mac*). *Download* program *PGP* gratis dari situs www.pgp.org atau www.pgpi.org (lihat Gambar 25.8).

- Kunci simetri hanya dipakai sekali (*one-time*) dan dibuat secara otomatis dari gerakan tetikus (*mouse*) atau ketikan tombol kunci.

- Kode sumbernya juga dapat diakses dari Internet. *PGP* terbaru adalah *PGP* versi 8. *PGP* versi-versi awal menggunakan *IDEA* sebagai algoritma simetri dan *RSA* sebagai algoritma kunci-publik (asimetri), sedangkan versi-versi terakhir menggunakan algoritma *CAST* sebagai algoritma simetri dan algoritam *DH* (Diffie-Hellman) sebagai algoritma kunci-publik.



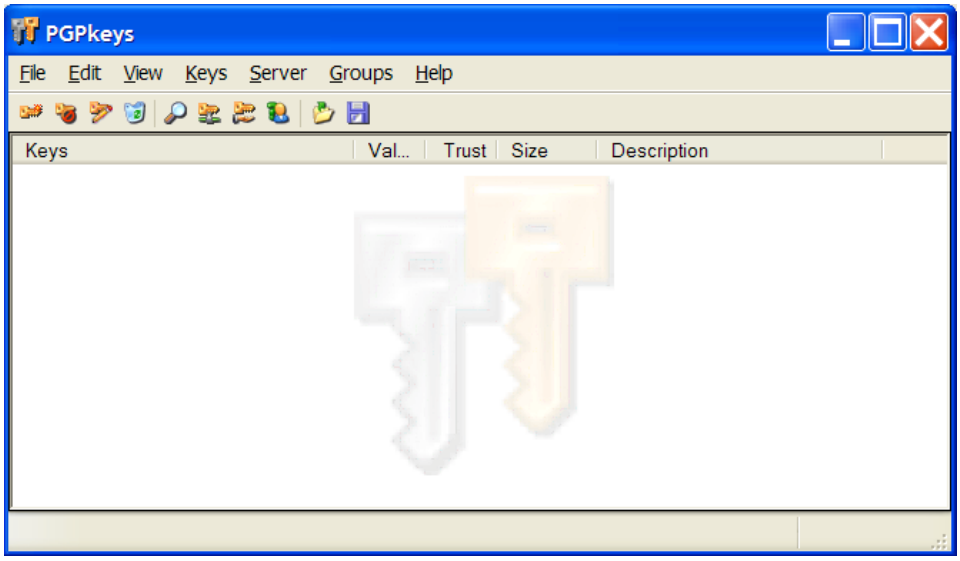
Gambar 25.8 Situs `www.pgp.com`

- *Download* dari situs *PGP* program *PGP* versi 8.0 *for Windows*, lalu instalasi PGP 8.0 ke dalam komputer anda.

- Pada versi *freeware* ini, ada tiga program *PGP* yang tersedia: *PGPdisk*, *PGPkeys* (pembangkitan dan manajemen kunci), dan *PGPmail* (enkripsi dan tanda-tangan digital untuk *file* maupun *e-mail*).

Membuat Pasangan Kunci Privat-Kunci Publik Baru

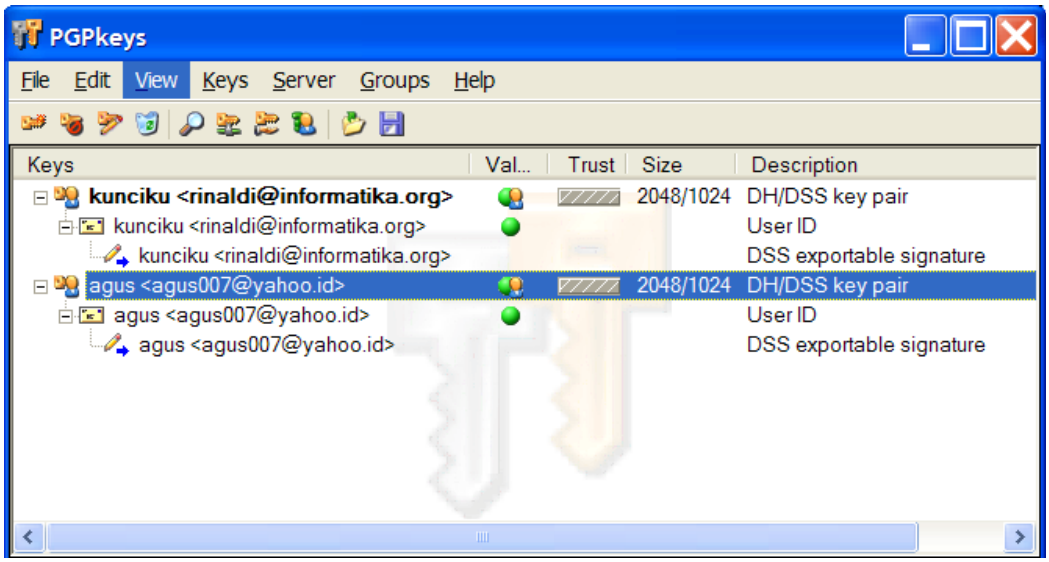
- Aktifkan *PGPkeys* sehingga muncul tampilan berikut:



- Pilih

  Keys → *New Key*

  selanjutnya akan ditampilkan *wizard* untuk membangkitkan pasangan kunci. Isilah beberapa isian yang disediakan.
  Contoh hasil pembangkitan beberapa pasangan kunci :



- Untuk melihat kunci publik, atau memberi kunci publik ke orang lain, ekspor kunci tersebut ke arsip (ekstensi arsip adalah `.asc`).

  Contoh kunci publik:

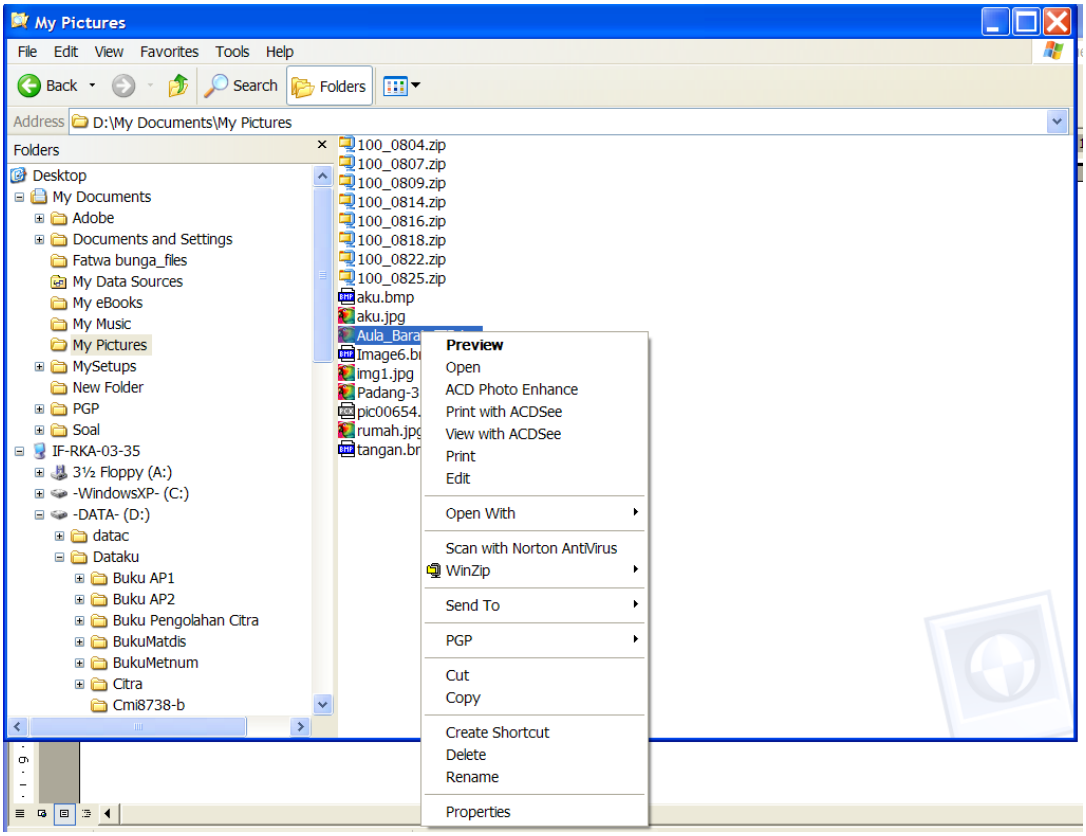
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.1 - not licensed for commercial use: www.pgp.com

mQGiBEHDmkIRBAD3p8b3phfk0FftdA2mRqEHLcg/iwF6VzcSde5ng9v86PeEB9xK
BMR9EiUjRdo1Us9YVi8awZ3iZG5EhX5sI/tbuBWJILCARhQzrn7Ww+sAuKrEPg4s
ggZtxYO1FsAbWhB/nKNqgDnYxxY3RbvOYlzH65Bk2xosR3H/YkHqc0L/SQCg/w0S
sh3fkWhymqao7rTJb4B/w2kD+QGWQlz81EkEbQaj3XeE4MdNMDjefKzxp/gP6I7Z
koJyiQxiIm1z4Q2R4iLniUX3hO7Vb9xre+J3s8D+rB0teJ70P7L2RNqK8QLVuqGh
lT1Yy4Okv5uuu0D4yTIOxB+vc3AlAoQwTVVSrKw5I8W7vaXvYBZd2m3w7ItDUjpP
uKhQA/9RjeQBq2QtBA2/7hLPP/NhSSfZ2C9A7rbN0ur3rG7mP0HB+hVFELR7tpW8
Mq+wPHP59qFlGWZpjR0E7svN96pLmQPW5x13Lc8Ip0D1z99o66vZ+UllRFNQR0kk
QO+V3kEIggWFpwOHi/Rz+vCVzrXRpR2CRSPinjxRswoC3vfnL7Qha3VuY2lrdSA8
cmluYWxkaUBpbmZvcm1hdGlrYS5vcmc+iQBdBBARAgAdBQJBw5pCBwsJCAcDAgoC
GQEFGwMAAAAFHgEAAAAACgkQFOUfEytY5dS/SwCg+wXNaoaVjnnMMsqUbF888cJF
WO0AoJWFiXP5yWfWqYSRXfqTAqYv0HGsuQINBEHDmkMQCAD2Qle3CH8IF3Kiutap
QvMF6PlTETlPtvFuuUs4INoBp1ajFOmPQFXz0AfGy0OplK33TGSGSfgMg71l6RfU
odNQ+PVZX9x2Uk89PY3bzpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV7H
AarTW56NoKVyOtQa8L9GAFgr5fSI/VhOSdvNILSd5JEHNmszbDgNRR0PfIizHHxb
LY7288kjwEPwpVsYjY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBgRjXyE
pwpy1obEAxnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1Xp
Mgs7AAICCADgUJgMdoFAmVvW3rwTmXtx78O6st/vPoUqMHlGcQeAJ6jFZNj9YzE6
Q5Z3rB6Prv41oTyGBTm/iHFKhluhuA5Zce66KpODlXEWWKesBETkdqMClrmXdBQY
Pff1+NDSpTFfEiJ8YtTz9h3qETCUKEe5u/9oh1e4xCPhjvDTbZKCLV9k7mFyw4Ma
hdRY3moH/3UkDQJD1pD0xdr60d52vMoW71tY2TQ/2tAEbVrRncp9dVXAoqSsOr+J
qRvc0KhP5/5P2u50BobzRJ1nGrlGfRhbI0gR18bZtNLfLDXpHGuMwreYeDxcnUUG
z1gmHb0Xbe/ymsBQoRPqPCdiYM0HDF//iQBMBBgRAgAMBQJBw5pDBRsMAAAAAAoJ
EBTlHxMrWOXUOlcAn3ehXWUDWkHSTW7q6gHpK44VMmpBAKClarHaLAUahiGhHNt2
AMaQYklN/Q==
=GLD1
-----END PGP PUBLIC KEY BLOCK---
```

- Kunci publik orang lain dapat dimasukkan ke dalam daftar kunci dengan cara memilih menu *Keys* → *Import*.

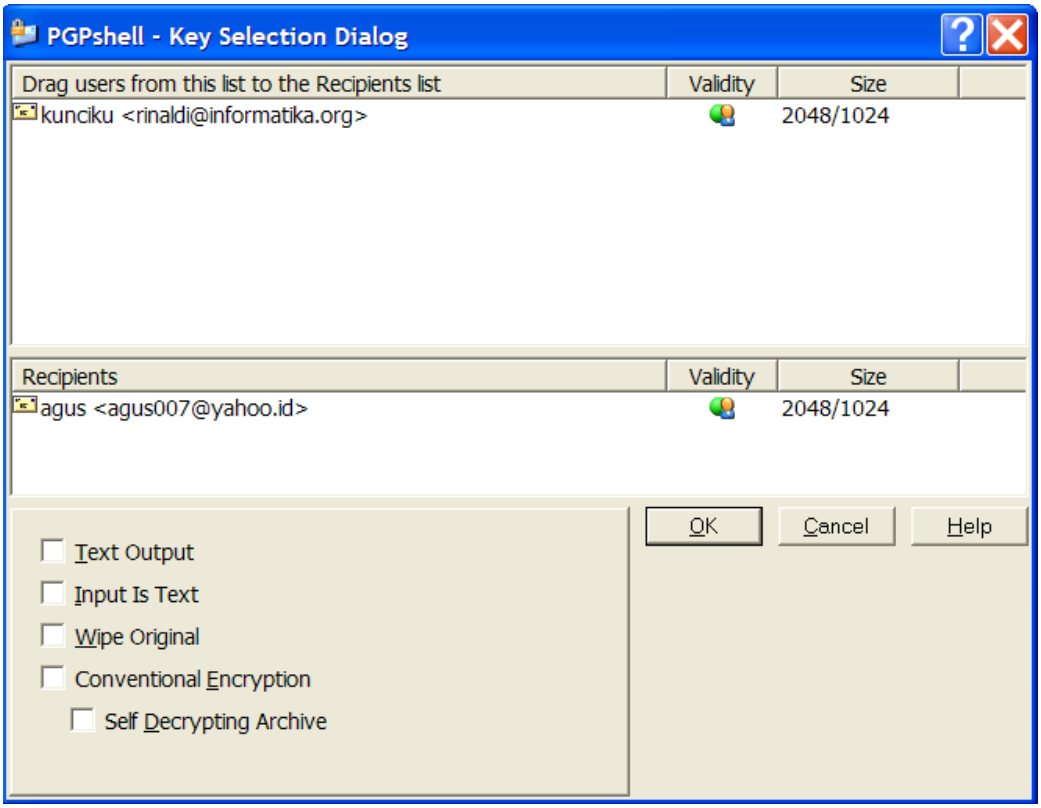
Mengenkripsi Arsip

(a) Mengenkripsi arsip yang akan dikirim

- Ada dua cara mengenkripsi arsip (*file*) yang akan dikirim
  1. Melalui *Windows Explorer*
     Pilih arsip yang akan dienkripsi, lalu klik kanan tetikus, dan pilih menu *PGP*.



Dari menu PGP, pilih *Encrypt*, sehingga muncul tampilan berikut:



Pilih *Recipents*(orang yang kita kirimi arsip), selanjutnya tekan *OK*. Arsip akan dienkripsi dengan kunci publik penerima.

Hasil enkripsi dapat dipilih untuk disimpan sebagai arsip teks (*Text Output* √) – dengan ektesni nama arsip `.asc` – atau sebagai arsip biner – dengan ekstensi nama arsip `.pgp`.

Contoh arsip `aula-barat.jpg` sebelum dienkripsi:

Arsip `aula-barat.jpg.asc` (*Text output*):

```
-----BEGIN PGP MESSAGE-----
Version: PGP 8.1 - not licensed for commercial use: www.pgp.com

qANQR1DBwU4Dj04oYGwvm0sQCADmCsgqnbpme3mDmoLCAp0lbHmeCtTR9dVQ0CZT
0P43mMkj7iR3F8pEaGOzeAsgj4YXy1iaYkZeUkujWuHeEbtZcjID9cRdOFy/jgNk
zvlSccANEhUcNRBqKCiZM/mesfUTOecXdMJ17T2ApsaMqjVxbHtDDnHGWlsX1Q5U
jysmIyZ9XcaCq9kJYGSK5u5yKYHAe9SQK8/dezYgfLKql//eNYK8ycwSYCzaNNBa
/ZdhAoydKuVCRaQmOROJJXYcI9A2MncjSrYXnELnJVykFM9sjn5xPptrLpybpJ4i
OyxzMzpaDCKAJ5De0lJDKWqGTY+FKwHnk9xmghn/2d5gYu+zB/4+69+UqrOW3jXU
Fna42wWPyWsZ8T5eJ3KvS6OZdIoP5NtT27iSwpJQWWm9X0BLEtv9pyddUWld7QE8
fy3wv+IgGMKLkh7ZgfgwckpBGao06LOHsyLk2YB2Jh25HSiszqqr0N112dhJbmd/
63R8WDtcfgNEh3IirAR6atZsOUPUJKzv6RC7ulQqxZHc3vL/dl+ElpujFOs50qs+
DSnofXvYPZYzrcCi0hS9IjRmPAQo1MwBgmNNpI1Tnp8A7gg09auSQEH3F4DEyEUB
t5s4SaEcJ0cZlt3Ps/HX1z1PTvkWJQbuJDsTVaZbL0KQosEt68EZWagMDGd25kBj
2fALpzoC0uwBkUOpPXtnTYvw/jafWXjtfogXeqHlN0cOu2mNb64S85RgLbv3q6V4
a0OSaLE9qNpSOnyqAibTxz1sKlChPZWwfu/ORkFdsgu4kFzLwXDCSEktWz2a9xJC
Uy5ybGALmRvPxQNMhX8b2JPb3fxtnBDrqRsMXnlgjXMR+8nmk57f6MuSEebyYscg
8PNKkTqKOXOMBc6ZPNOh4ZxnPzHZrsgHvLgbdudie3p9uIFVTEoi5V2qj5O5/oy+
kYgJg+ix+R28zA33iFIFhN7PTfWwuFIlgOpk+7cLr+KDl8TKnzIgfrKdzXYNjErl
jrtZ8ws5JMPDwAgQ6677dUq1i1g3P2zXJwmgsdF9A4uC2JvpJeCbKu3Sy6ZXP4CX

... (deleted, because too long)

-----END PGP MESSAGE-----
```

Untuk mendekripsi arsip, klik arsip yang terenkripsi, selanjutnya klik kanan tetikus, dan pilih *Decrypt*. Program *PGP* meminta anda memasukkan *passphrase* untuk kunci privat (harus sama dengan passphrase yang diisikan pada waktu pembangkitan pasangan kunci).

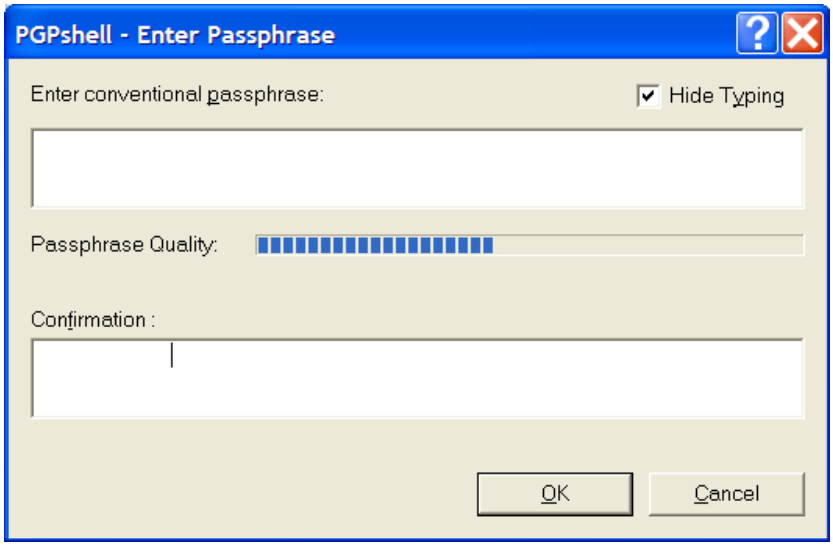
Jika *passphrase* benar, maka arsip akan didekripsi dengan menggunakan kunci privat yang berkoresponden dengan kunci publiknya.

2. Melalui program *PGPmail*
   Aktifkan program *PGPmail*, sehingga muncul tampilan berikut:

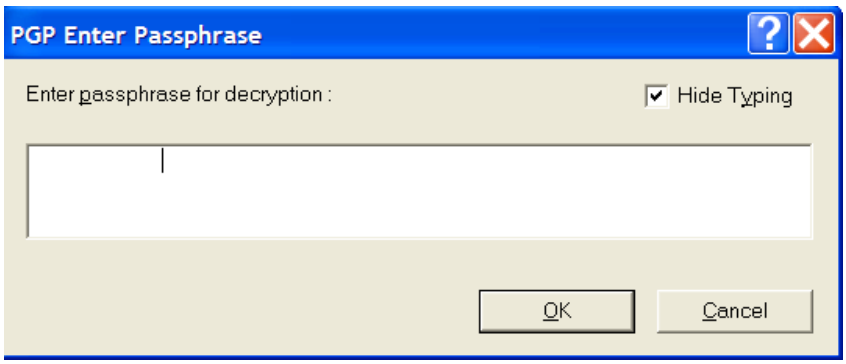
Pilih ikon surat+gembok, dan selanjutnya tahapan enkripsi sama seperti cara pertama.

(b) Mengenkripsi arsip dengan algoritma simetri

Jika opsi *Conventional Encryption* dipilih, maka arsip akan dienkripsi dengan algoritma simetri. Di sini kunci simetri dibangkitkan dari *passphrase* yang diketikkan oleh pengguna:



Untuk mendekripsi arsip, klik arsip tersebut, lalu klik kanan tetikus, pilih menu PGP, lalu pilih *Decrypt*:



Ketikkan *passphrase* yang sama seperti waktu enkripsi. Hasil dekripsi dapat disimpan dengan nama lain.

Contoh enkripsi arsip `bandung.txt`.

(i) Arsip `bandung.txt` sebelum dienkripsi

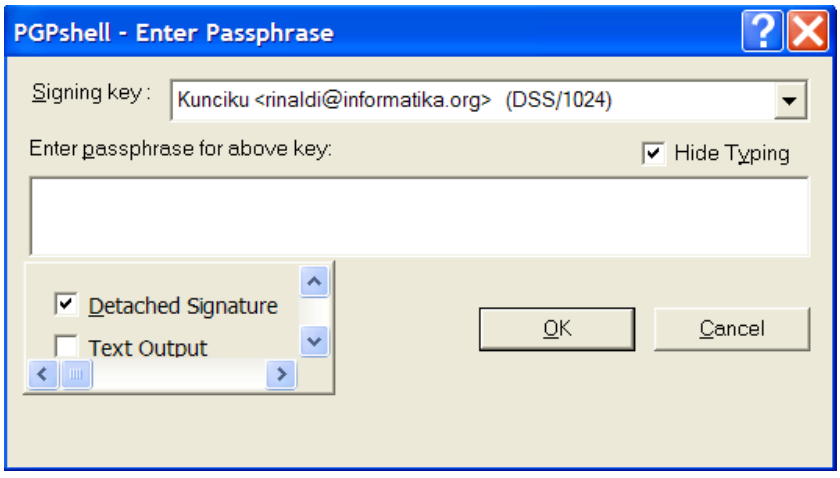
```
Pada bulan Oktober 2004 ini, suhu udara kota Bandung terasa lebih
panas dari hari-hari biasanya. Menurut laporan Dinas Meteorologi
Kota Bandung, suhu tertinggi kota Bandung adalah 32  derajat
Celcius pada Hari Rabu, 17 Oktober yang lalu. Suhu terseut sudah
menyamai suhu kota Jakarta pada hari-hari biasa. Menurut Kepala
Dinas Meteorologi, peningkatan suhu tersebut terjadi karena
posisi bumi sekarang ini lebih dekat ke matahari daripada hari-
hari biasa.

Sebutan Bandung sebagai kota sejuk dan dingin mungkin tidak lama
lagi akan tinggal kenangan. Disamping karena faktor alam, jumlah
penduduk yang padat, polusi dari pabrik di sekita Bandung, asap
knalpot kendaraan, ikut menambah kenaikan suhu udara kota.
```

(ii) Arsip `bandung.txt.asc` setelah dienkripsi

```
-----BEGIN PGP MESSAGE-----
Version: PGP 8.1 - not licensed for commercial use: www.pgp.com

qANQR1DDDQQJAwKRt3ROh/zvkWDSwQ8BSzulggHt+bRY/Ma3X/0iEnhSh4xs/q14
m7KjXHi0c7EoQnGvfhZiEA5lzASdqVpUkdR0bRI4F/Vn8D4RWqmmca1qm7KskqRo
+wenFvfQYGBeagM1WOWTrWBKJAPdVG88oCcOE97Bf5YC+Z5f57PAjp5CgrHXj09N
4ElNR2EHohBzhOEAGYIzzzxNBS4kUD8XdThUBqlKSqRO8ZxZora20qYc1oHe79TC
+4T5BG+B+AUCQsTGx8zL2GwoCF/r1ed2SldTJou952gLMpMa6BPvn37VFs1s7EUG
zXa56peaq+bPMYZYW8J69OeoIdDjX6avrbsVOpk07mbOBQl2XbpteKFBz+fjldYE
8MrWblaGL26Q0feoHhckwVsa5uiUrFkjG6mQQubddibenWFMkp64jhDtgyXLJUUi
onFyQsQCFAxQUrcDRw4/0ggmq+qgBtSD4mg2AhhsQCleNbAqWO72yVJcX73eHZ1M
b8NTCMwrsKfMxEs35tY1OU1/SKvi4DlqOgNb5ye0oTzKcpzgJBuk82yJOJFnXkaW
NUysrLONu0kgC/UI3Ma4mtBOAxk4TjNfmEZWmHcI0cDTQ2/FFto8gNxP54qveFB0
IRj8qcpf
=6oEr
-----END PGP MESSAGE-----
```

Memberi Tanda-tangan

- Pilih arsip yang akan ditandatangani, lalu klik kanan tetikus, dan pilih menu *PGP*, kemudian pilih *Sign*.



Arsip akan ditandatangani dengan kunci privat. Masukkan *passphrase* untuk kunci privat. Tandatangan dapat disimpan terpisah menjadi arsip khusus (ekstensi `.sig`) atau digabung menjadi satu dengan arsip (*Detached Signature* √).

Contoh penandatanganan arsip `bandung.txt`.

(i) Arsip `bandung.txt` sebelum ditandatangani

```
Pada bulan Oktober 2004 ini, suhu udara kota Bandung terasa lebih
panas dari hari-hari biasanya. Menurut laporan Dinas Meteorologi
Kota Bandung, suhu tertinggi kota Bandung adalah 32  derajat
Celcius pada Hari Rabu, 17 Oktober yang lalu. Suhu terseut sudah
menyamai suhu kota Jakarta pada hari-hari biasa. Menurut Kepala
Dinas Meteorologi, peningkatan suhu tersebut terjadi karena
posisi bumi sekarang ini lebih dekat ke matahari daripada hari-
hari biasa.

Sebutan Bandung sebagai kota sejuk dan dingin mungkin tidak lama
lagi akan tinggal kenangan. Disamping karena faktor alam, jumlah
penduduk yang padat, polusi dari pabrik di sekita Bandung, asap
knalpot kendaraan, ikut menambah kenaikan suhu udara kota.
```

(ii) Arsip `bandung.txt` setelah ditandatangani

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Pada bulan Oktober 2004 ini, suhu udara kota Bandung terasa lebih
panas dari hari-hari biasanya. Menurut laporan Dinas Meteorologi
Kota Bandung, suhu tertinggi kota Bandung adalah 32  derajat
Celcius pada Hari Rabu, 17 Oktober yang lalu. Suhu terseut sudah
menyamai suhu kota Jakarta pada
hari-hari biasa. Menurut Kepala Dinas Meteorologi, peningkatan
suhu tersebut terjadi karena posisi bumi sekarang ini lebih dekat
ke matahari daripada hari-hari biasa.

Sebutan Bandung sebagai kota sejuk dan dingin mungkin tidak lama
lagi akan tinggal kenangan. Disamping karena faktor alam, jumlah
penduduk yang padat, polusi dari pabrik di sekita Bandung, asap
knalpot kendaraan, ikut menambah kenaikan suhu udara kota.

-----BEGIN PGP SIGNATURE-----
Version: PGP 8.1 - not licensed for commercial use: www.pgp.com

iQA/AwUBQcOWFJTpyRekJ1FcEQI8xgCaAmBME/O/lIOfdvZZUfnHcgdhHPAAoPxJ
WPpSilIHIl63h3/iHoB9fIc2
=eKHn
-----END PGP SIGNATURE-----
```