안전한 메일, 파일 전송 및 보관

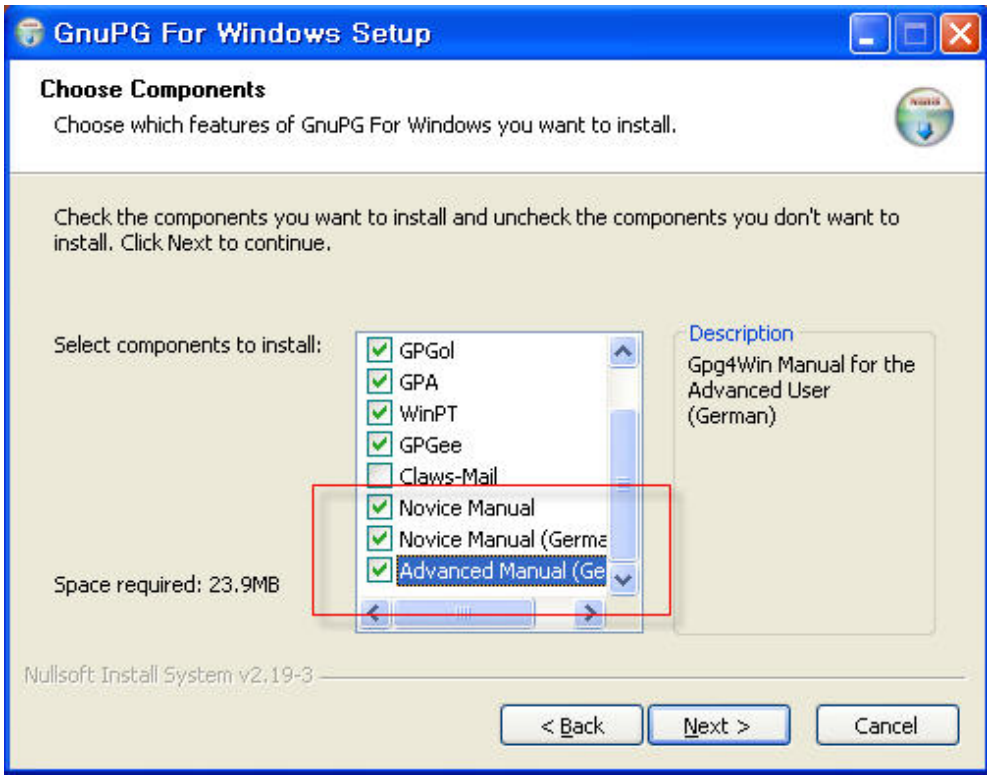
By vangelis(securityproof@gmail.com)

요즘 메일을 통해 중요한 파일을 전송하는 일이 많아졌다. 그리고 무료 메일 계정을 제공하는 곳도 점차 증가하고 있다. 그러나 그 무료 계정이 보안과 개인 프라이버시를 보장해주지는 않는다. 이 글에서는 메일을 안전하게 보내는 방법과 파일을 더욱 안전하게 전송하는 것에 대해 알아보기로 한다. 심지어 자신의 중요한 파일을 안전하게 저장하는 방법이 될 수도 있다.

이 글에서는 gpg4win이라는 프로그램을 소개할 것이다. gpg4win은 GnuPG(http://gnupg.org/)의 Windows 버전이다. GnuPG는 RFC8440에 정의되어 있는 OpenPGP 표준을 구현한 것이다. GnuPG는 데이터와 커뮤니케이션을 암호화할 수 있고, GPG로도 알려져 있다.

http://www.gpg4win.org/ 에 가서 Gpg4win 최신 버전을 다운받는다. Gpg4win light 버전도 있으나 매뉴얼과 GnuPG2 커맨드 라인 툴이 생략되기 때문에 light 버전보다는 Gpg4win 버전을 다운받기를 권한다. 이 글을 작성하는 현재 1.1.3 버전이 가장 최신 버전이다.

먼저 설치부터 하자. 본격적인 설치 단계에서 초보자들과 상세한 매뉴얼을 선택하는 부분이 있는데, 이 부분은 필요한 사람들만 선택하면 되겠다. 자세한 매뉴얼이 필요하다면 Novice Manual 부분만 제외하고 설치하자.

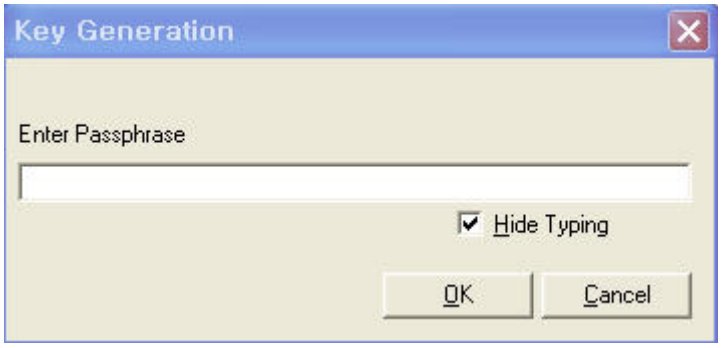


나머지 부분은 어려움 없이 설치할 수 있을 것이다.

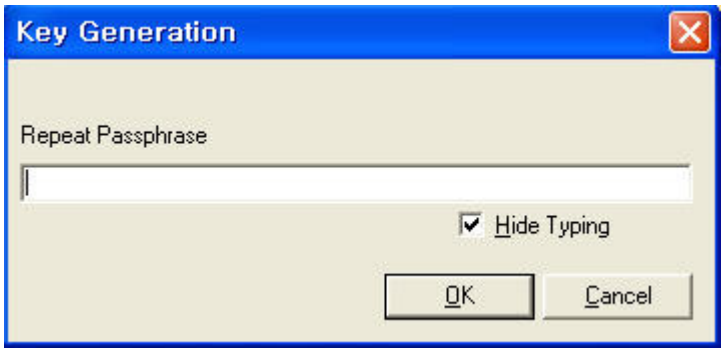
설치가 끝난 후 WinPT를 클릭하면 다음과 같은 스크린이 등장한다.

여기서 OK 버튼을 클릭한다. 클릭하면 다음과 같은 스크린이 등장한다.

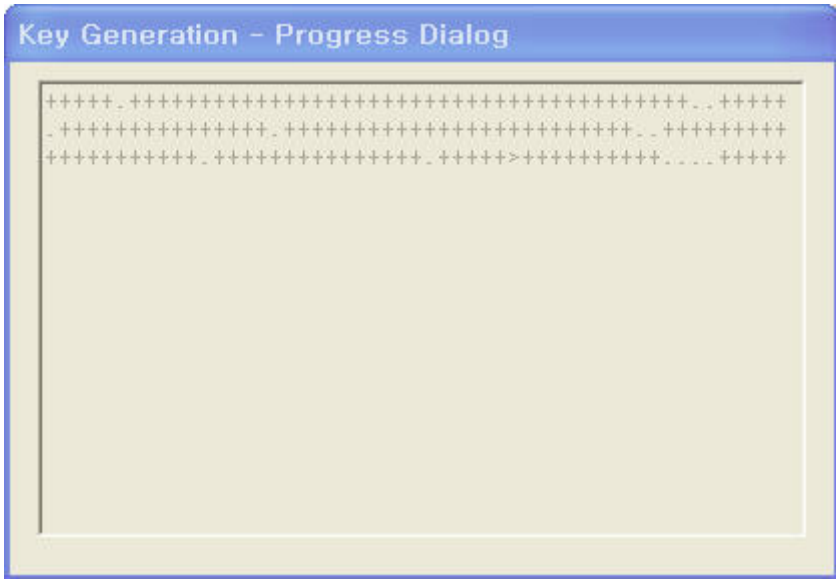
여기서는 **공개키(public key)를 만드는 과정**이다. 이 키는 E-mail 뿐만 아니라 파일 전송을 위해서도 필요하다. 여기서 Real name 부분에 굳이 실제 자기 이름을 넣을 필요는 없다. E-mail address 부분 역시 자신이 사용하는 e-mail 주소를 입력하면 되는데, 단순히 파일 전송이 목적이라면 굳이 정확한 e-mail 주소를 입력할 필요는 없다. RSA key를 선호한다면 Prefer RSA keys 부분을 체크한다. 입력이 끝나고 OK 버튼을 클릭하면 다음과 같은 창이 뜬다.



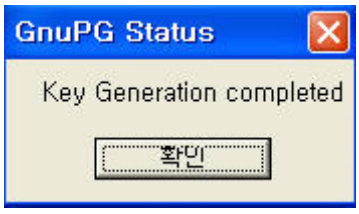
여기서는 passphrase를 입력한다. 이 패스워드는 자신만이 알고 있어야 할 부분이다. 입력하고 OK 버튼을 클릭하면 다시 한번 더 passphrase를 입력한다.



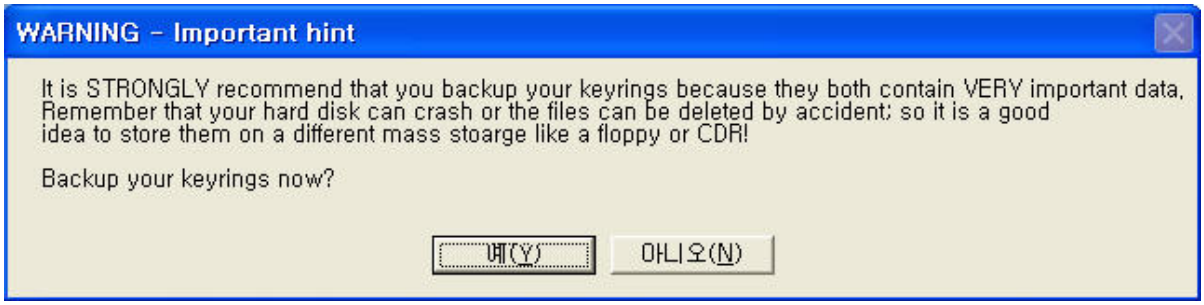
OK 버튼을 클릭하면 Key 생성 과정이 나온다.



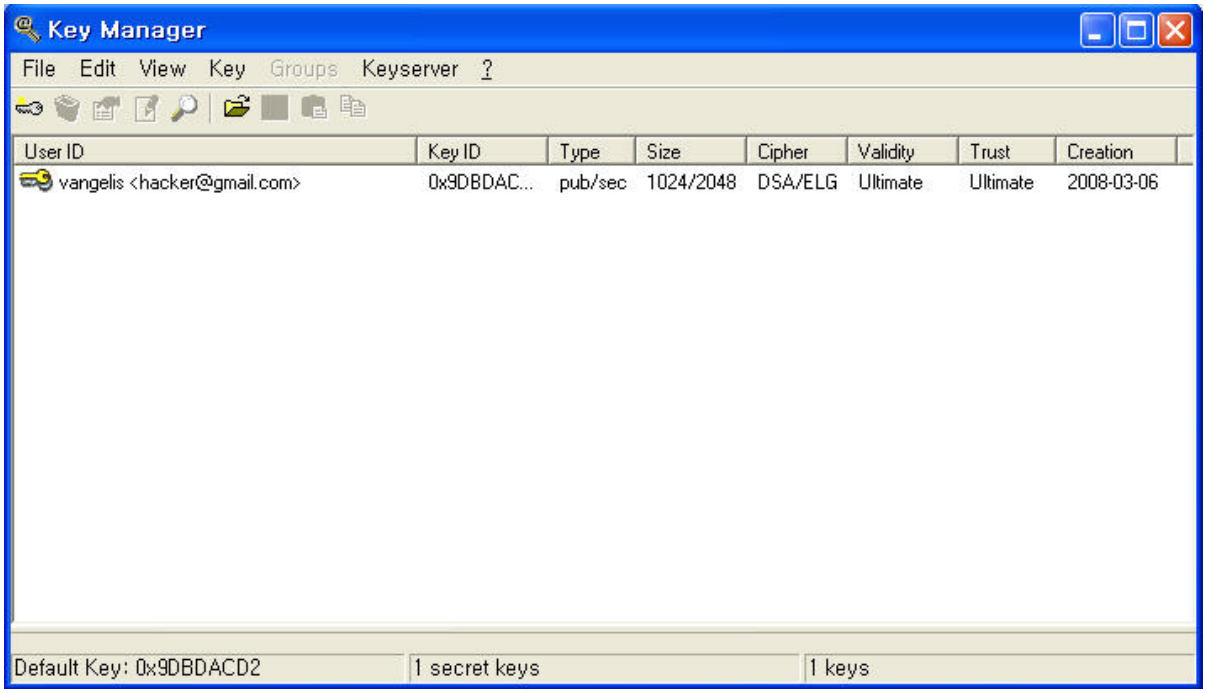
Key 값이 생성되면 완료되었다는 창이 뜨고, OK 버튼을 클릭한다.



OK 버튼을 클릭하면 keyrings를 백업할 것인지를 묻는데, 예(Y) 클릭한다.



백업 과정이 끝나면 다음과 같은 Key Manager의 창이 뜬다. 백업 파일은 C:₩Program Files₩GNU₩GnuPG₩share에 저장된다.



이제 public key를 생성하는데 성공했다.

이제 생성된 public key를 추출한다. 먼저 Key Manager의 메뉴바에서 Key를 클릭한 후 export를 다시 클릭한다. 그러면 asc 파일로 저장하게 된다. 만약 key 생성 초기에 Real name을 vangelis라고 했다면 vangelis.asc라는 이름으로 저장된다. 이 파일 역시 C:₩Program Files₩GNU₩GnuPG₩share에 저장된다. 저장된 파일을 메모장으로 읽으면 다음과 같이 PGP Public Key를 확인할 수 있다.

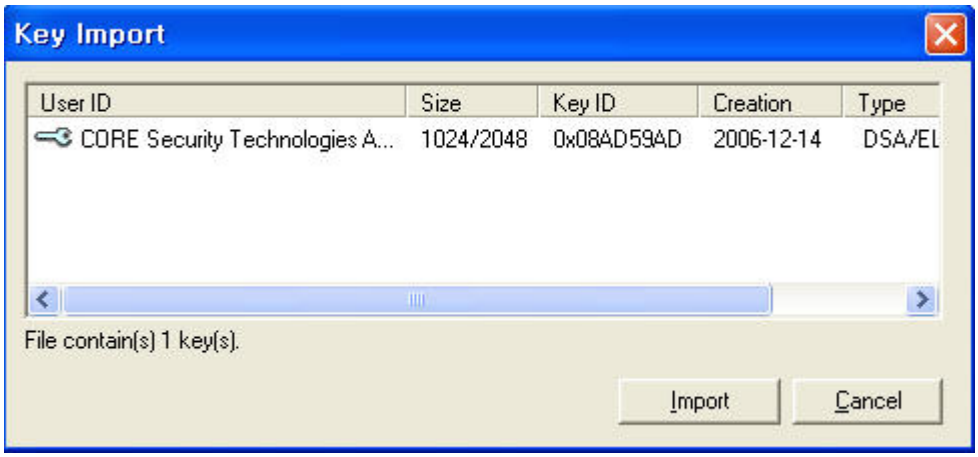
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.7 (MingW32)

mQGiBEfOt3wRBACZyudxJMIMODGqOth9mxsKbn20qc9xtQkUEM5FL721Rjv5Zp+u
e5Ra0UfW+ulrKDRLEayXg0vuS1E3YOCjxjGYKJt4uzH1B6B3CrNtNBgtZAKKw3iX
V816xE9WuuHNB2eHPz4aKvQHMDQgxrIT0Bx8G5+uASAjSPy7z5OFoW58fwCgn78T
jmY9g0HFCVZoVz6zzobmH70D/0/PE0McTQMvSwd1U00fF0aPqugBdjL5iDfN9FHu
QEzerOl8khNhqO8ugbPZqsn009Q55Cxw9t7kRb9DMq7loc2+p34TtURBk1SNnqvo
SzOjdYG97NQQK+/NETrQnCHZzxcVU7fW31F3/sW1Qv8NyOvgHgXHdjcLTmpCnRHe
S3l/A/sGZfkZZKrs2+fRTqgsFEqkZMNngynPFEMCSbzlEEb/cNUXYJSrTuXcCmLm
Ynpi2K6dE2Q+IiXYWSS3TFl/78sbGXpJC/B6Zm9/xQ03QZsjPba6HJB4jXw/tj2Q
CJELgU7eqdJIrKP5yKaNoBGNZr9dtPxbvkKaYkHOKf7qwsU43bQbdmFuZ2VsaXMg
PGhhY2tlckBnbWFpbC5jb20+iGAEExECACAFAkfOt3wCGwMGCwkIBwMCBBUCCAME
FgIDAQIeAQIXgAAKCRABkElknb2s0vHJAJ40cHDNWCr0/F/H8RVCldr5kROvDQCd
GVlhByuCBnNH0F4w4tfn24d3gkK5Ag0ER863fBAIALPXGTi1t6N/PXR2PqHbGO5K
XRnw4R+K2L+rTlK1y7I9GWiMFXTRGmJRxL2eSsdgEib0X8Vf/EG6WJh9SzEmcxi1
SQfw2RkikrJxlZmrjau5xFwijYZ2cgsHcdwqtloMZ7SHdCpXCbF2/+ZhtgGoGzWN
OPhujscrvXybm2DnIGbG2CZgFOeeFrF/UXrymt85EbCjr6cteLINAN3v0EYwB6UO
XXtN7e2s/2dG0GQzZczMBIRhzOli2v0oEmXjVg3iQivd9m5wto9P73K/LiIVGGoe
9M4V2+ftcmmqA/s98JpmGGddWhrcjlgW2fSl4px/4tzZqsua15jvt36ZPQlT+hMA
AwUH/2Nc5+HuQTnNXm/sXGZwdpFBpbQFCs/975XFGfKDiParReT3WOHQC00uO7DS
wbde52sci8NtNg9QFN2+A32zHHM2G0q3l/4m51xYYvBoxZ9yJFylJnSO0EMyjNhy
```

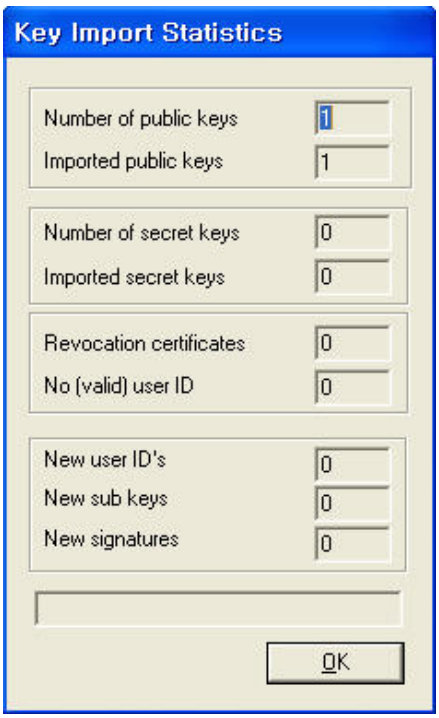
```
4ScZzrXSukgQ2ILdfB8IGsecVQ3J5esQWUBDoXsYEc5Lx0b/GAooLRUksVwNJQuO
7aZKYJeimXaaJNgVBhrMadPglgosRPNSvhnB0sWm+fxCpjYu5xMiXnJl1s1katch
X2I2e1gKkM8kpMs8OKjzEEiICn0U4jjFgUDxXwPu3t/Y/tI6fAASyTr/IpRlLW5C
4Zz/SlvtT6Or3n1euU6O+0n91x+ISQQYEQIACQUCR863fAIbDAAKCRABkElknb2s
0uN9AJ4mBng5HGI52Heru6L5jdCszOPRPACcDAfHs/MPrSAe2Q2mVbiKs0dA/Dk=
=pyyJ
-----END PGP PUBLIC KEY BLOCK-----
```

이 asc 파일을 e-mail이나 파일을 주고 받을 다른 사람들에게 제공하면 된다. 상대방도 같은 방식으로 asc 파일을 전달한다.

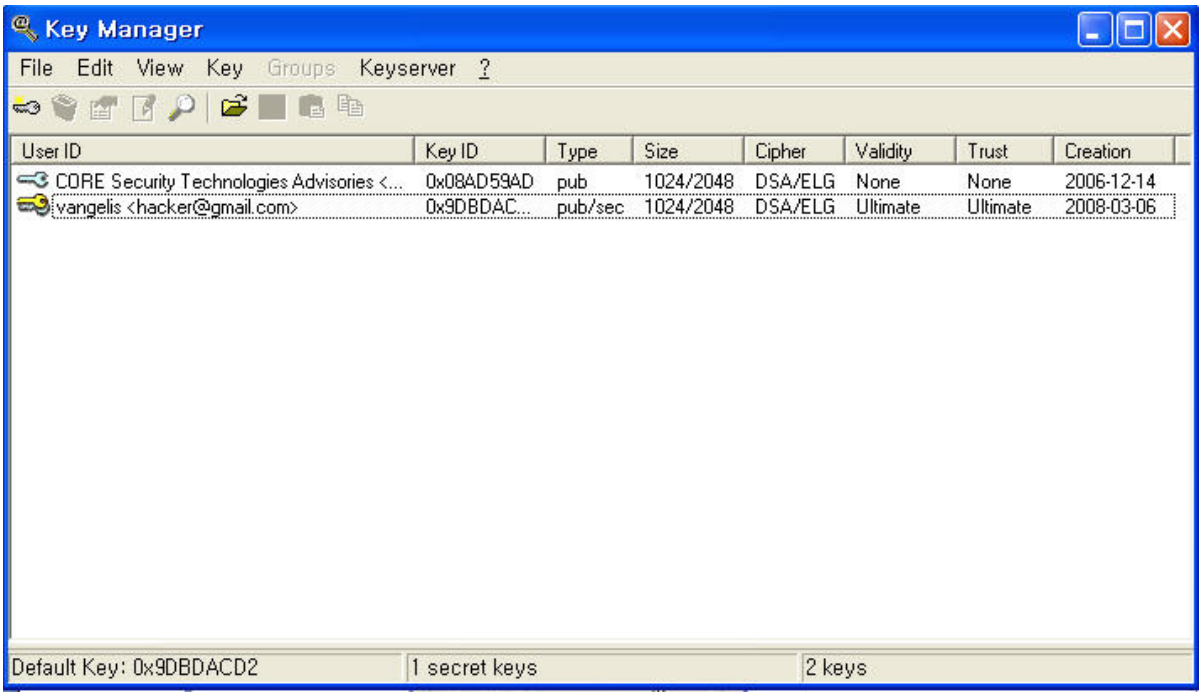
이제 상대방의 public key를 등록해야 하는데, 그 방법은 아주 간단하다. 상대방으로부터 asc 파일을 받아 Key Manager로 끌어 놓으면 된다. 이 글에서는 메일링 리스트에 올라온 CORE Security Technologies의 asc 파일을 설명을 사용했다. asc 파일을 끌어두면 다음과 같은 창이 뜬다.



여기서 import를 클릭하면 다음과 같은 창이 뜬다.

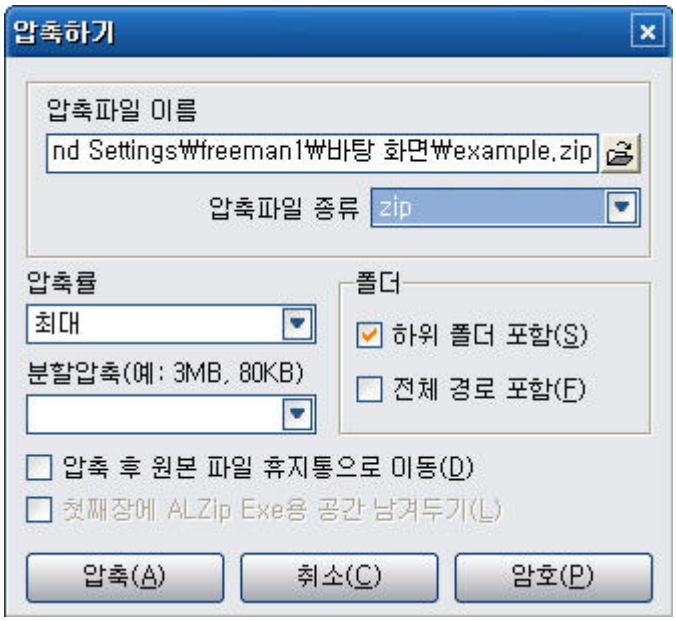


여기서 OK를 클릭하면 다음과 같이 상대방의 key 값이 등록된다.



이제부터는 활용 방법에 대해 알아본다.

먼저 상대방에게 파일을 전송하는 것에 대해 알아보자. Example.txt라는 파일을 상대방에게 전송할 것이다. 내가 만든 example.txt라는 파일이 조작 없이 안전하게 전달되게 하는 것이 목적이다. 보안을 위해 먼저 파일을 압축하는데, 압축할 때 패스워드를 지정하면 안전할 것이다.



필자는 알집을 이용하는데, 오른쪽 아래를 보면 압축 시 암호를 입력하는 부분이 있다. 이 부분을 이용해 암호를 지정하고 압축을 하자. 암호를 지정할 때는 최소 8자 이상의 조합을 사용한다. 압축 시 파일 포맷은 여러분들이 선택하길 바란다. 여기서 지정한 암호는 상대방도 알고 있어야 한

다. 모를 경우 gpg 파일을 decrypt 한 이후에도 압축된 파일을 볼 수 없을 것이기 때문이다.

암호를 지정한 후 압축이 완료되면 압축된 파일 위에 마우스를 위치시키고, 오른 마우스를 클릭한다. 그런 다음 열쇠 표시와 함께 있는 GPGee에 마우스를 올리면 다시 메뉴창이 뜨는데, 여기서 Encrypt(PK) 부분을 클릭한다. 그러면 Sign/Encrypt 창이 뜨는데, 이때 상대방의 공개 키 부분을 체크한 후 OK 버튼을 클릭한다. 그러면 example.zip.gpg 파일이 생성된다. 앞에서 예를 들었든 example.zip파일은 example.zip.gpg와 같이 생성된다.

그 다음 이 gpg 파일을 상대방에게 전달하는데, 전달할 때는 세 가지가 있을 것이다. 직접 전달하거나, 아니면 e-mail 또는 메신저와 같은 p2p 프로그램을 이용하는 것이다. 여기서는 e-mail을 이용할 때와 메신저를 이용하는 것에 대해 간단하게 알아보자.

요즘 gmail과 같은 무료 계정을 이용하는 사람들이 많을 것이다. 그런데 이 무료 계정들이 완벽한 프라이버시나 보안을 담보해주지 않는다. 어떤 경우 메일 서버에 보관될 수도 있다. 그래서 메일을 보낼 때는 메일의 실제 내용은 압축 파일 안에 포함시켜 gpg 파일을 첨부 파일로 보내는 것이다. 이럴 경우 악의적인 공격자가 내 메일 계정을 크래킹하여 파일을 갈취하더라도 파일의 내용을 쉽게 볼 수 없을 것이다.

gpg 파일로 변환한 것을 메신저로 보내는 것도 한 방법이다. 왜냐하면 서버에 저장되는 것을 막을 수 있기 때문이다.

이런 식으로 사용한다면 Key 값을 생성할 때 정확한 이름과 e-mail 주소를 입력할 필요가 없을 것이다. 상대방도 같은 순서로 하면 된다. 상대방은 나의 asc 파일을 이용해 암호화한다. 이제 파일을 받았다면 이 파일의 암호를 풀어 파일의 내용을 확인하는 방법에 대해 알아보자.

먼저 상대방으로부터 받은 파일에 마우스를 올리고 오른쪽 마우스를 클릭하여 GPGee에 마우스를 올리면 **Verify/Decrypt**를 선택한다. 그러면 **Enter Passphrase** 창이 뜨는데, 이때 key 값을 생성할 때 사용한 passphrase를 입력한 후 OK 버튼을 클릭하면 다음과 같은 성공 메시지가 뜬다.

Successfully decrypted and written to file "C:\Documents and Settings\hacker\바탕 화면\example.zip".

마지막으로 자신의 컴퓨터에 있는 파일들을 안전하게 보관할 때 gpg4win를 활용하는 방법은 없을까? 있다. 바로 앞에서 설명한 것과 하나만 차이가 있을 뿐이다.

최초 자신의 public key를 만들었을 때 그 key를 이용해 암호화하는 것이다. 즉, GPGee를 이용해 자신의 public key로 암호화 하고, 다시 GPGee를 이용해 자신의 public key의 passphrase를 이용해 해독하면 된다.

그런데 다른 사람의 public key 값을 등록하면 GPGee를 통한 자신의 public key로 암호화가 되지 않는 문제가 gpg4win에 있는 것 같다. 처음부터 의도한 것인가?