그누 사생활 지킴이를 만나보세요

envia, 컴퓨터를 배우는 학생
http://envia.pe.kr/, http://blog.jinbo.net/envia/

2008년 5월 20일

요약

이 문서는 윈도 환경에서 GnuPG(GNU Privacy Guard, 그누 사생활 지킴이)를 이용하여 이메일과 파일의 내용을 암호화하고 푸는 방법을 설명합니다.

강조

비밀 열쇠와 비밀문구는 소중한 것입니다.

1 소개

1.1 GnuPG는 무엇인가

GnuPG는 문서와 파일의 내용을 암호화할 때 사용하는 프로그램입니다.

이름에 대해 조금 더 알아보면, GnuPG(그누피지)는 GNU Privacy Guard를 줄인 이름입니다. 더 줄여서 GPG(지피지)라고 부르기도 합니다. GNU Privacy Guard는 보통 그누 사생활 경비원으로 옮기는데, 그누 사생활 지킴이라고 부르는 것이 더욱 친근할 것 같습니다.

1.2 암호화는 무엇인가

암호화는 어떠한 정보를 알아볼 수 어렵게 만드는 것을 말합니다. 사실 그냥 알아보기 어렵게 만드는 것은 아닙니다. 비밀번호를 가진 사람은 쉽게 알아볼 수 있지만, 그렇지 않은 사람은 알아보기 어렵게 만듭니다. 비밀번호를 가진 사람이 암호화를 해제해서 암호화된 정보를 원래 정보로 돌려놓는 것을 **복호화**라고 합니다. 암호화를 하고 해제하는 것이 자물쇠로 잠그고 열쇠로 여는 것과 비슷하므로 비밀번호를 **열쇠**라고 부릅니다.

암호화와 복호화를 하는 방법에는 크게 두 가지가 있습니다. 첫 번째 방법은 **대칭 암호**입니다. 대칭 암호는 열쇠가 하나이고, 암호화를 할 때와 해제할 때 같은 열쇠를 사용합니다. 예를 들어 비밀번호 "1234"로 이메일을 암호화해서 보냈다면, 상대방은 "1234"를 이용해서 암호화를 해제할 수 있습니다. 대칭 암호에서 쓰는 열쇠를 비밀 열쇠라고 부르기도 합니다.

대칭 암호는 혼자서 사용하거나 자주 만나는 사람과 사용할 때에는 괜찮지만, 쉽게 만나기 어려운 사람과 사용할 때에는 문제가 있습니다. 비밀번호 "ABCD"로 이메일을 암호화해서 보냈다고 합시다. 상대방이 이메일을 읽을 수 있도록 하려면 비밀번호를 전달해 주어야 하는데, 안전하게 비밀번호를 전달하기가 쉽지가 않습니다. 비밀번호를 이메일로 전달하면 기껏 암호화한 것이 의미가 없어집니다. 누군가가 이메일을 가로챈다면 이메일에 있는 비밀번호를 이용해서 암호화된 이메일을 읽을 수 있기 때문입니다.

그래서 나온 것이 두 번째 방법인 **공개 열쇠 암호**라고도 하는 비대칭 암호입니다. 비대칭 암호에서는 열쇠가 두 개입니다. 하나는 **공개 열쇠**이고, 다른 하나는 **개인 열쇠**라고도 하는 비공개 열쇠입니다. 하나로 암호화한 것은 다른 하나로 해제할 수 있지만, 하나를 이용해서 다른 하나를 알아내는 것은 어렵게 설계되어 있습니다. 예를 들어 공개 열쇠가 "ABCD"이고 비밀 열쇠가 "1234"라면, "ABCD"로 암호화한 것은 "1234"로 해제할 수 있고, "1234"로 암호화한 것은 "ABCD"로 해제할 수 있지만, 공개 열쇠가 "ABCD"라는 것을 이용해서 비밀 열쇠가 "1234"라는 것을 알아내는 것은 어렵게 되어 있습니다. 개인 열쇠는 개인이 가지고 있고, 공개 열쇠는 아무나 알 수 있도록 공개해 놓습니다. 공개 열쇠 암호를 이용해서 이메일을 보낼 때에는 상대방의 공개 열쇠를 이용해서 암호화를 합니다. 그러면 상대방은 자신의 개인 열쇠를 이용해서 암호화를 해제하고 내용을 읽을 수 있습니다.

나의 비밀 열쇠로 암호화를 하는 경우도 생각해 봅시다. 이때 상대방은 나의 공개 열쇠를 이용해서 암호를 해제할 수 있습니다. 나의 공개 열쇠는 아무나 알 수 있도록 공개되어 있기 때문에 암호화의 효과는 거둘 수 없지만, 나의 비밀 열쇠로 암호화한 것만 나의 공개 열쇠로 암호화를 해제할 수 있기 때문에 상대방은 이메일을 보낸 사람이 나의 비밀 열쇠를 가진 사람인 나 자신이라는 것을 알 수 있게 됩니다. 이는 편지에 서명해서 내가 보낸 편지라는 것을 증명하는 것과 비슷하므로 **서명**이라고 합니다.

GnuPG가 한글화가 되어 있지 않기 때문에 영어 용어들도 함께 알아 두시면 좋겠습니다. 암호화는 **encryption**, 복호화는 **decryption**, 서명은 **signature**입니다. 그리고 "암호화하다"는 **encrypt**, "복호화하다"는 **decrypt**, "서명하다"는 **sign**이 되겠습니다.

1.3 암호화는 왜 하는가

비밀 정보를 주고받는 데 필요합니다. 비밀 정보라고 하니 무엇인가 대단한 것 같지만, 사실 그렇지만은 않습니다. 개인적으로 주고받는 이메일에 담겨 있는 내용이 새어 나가지 않기를 바란다면 비밀이라고 할 수 있습니다. 업무와 관련되어 주고받는 자료들도 다른 사람들이 보기를 원하지 않는다면 비밀이라고 생각할 수 있습니다.

정보화가 진행되면서 점점 더 많은 정보가 컴퓨터와 인터넷에 보관되고 있고, 이러한 정보들을 보호하기 위해 나름대로 조치들을 취하지만, 아주 중요한 비밀들을 저장하기에는 부족할 때도 있습니다. 어떤 업체들은 광고에 출력할 내용을 결정하기 위해 이메일에 담겨 있는 내용을 분석하기도 합니다. 대형 업체의 서버가 해킹을 당하기도 하고, 개인 컴퓨터의 경우 도난의 위험까지 있습니다. 암호화를 이용하면 정보가 유출되더라도 해독이 어려우므로 비밀과 프라이버시를 지킬 수 있습니다.

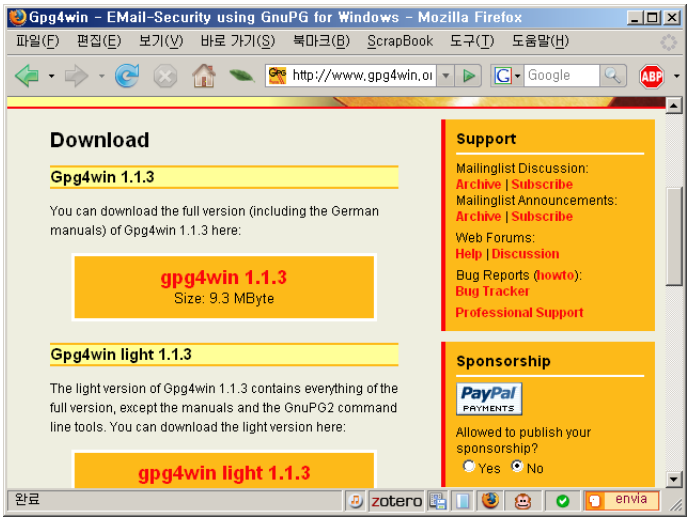
2 설치하기

GnuPG를 설치하고 사용하는 것은 생각보다 간단합니다. 여기에서는 윈도에서의 설치 방법을 다루어 보겠습니다. 다른 환경에서는 참고 자료에 있는 문서들을 이용하실 수 있습니다.

2.1 내려받기

윈도 환경에서는 Gpg4win을 이용해서 설치하시면 됩니다. Gpg4win에는 GnuPG와 GnuPG를 편리하게 사용할 수 있도록 돕는 프로그램들이 함께 들어 있습니다. **http://www.gpg4win.org/**에서 내려받으실 수 있습니다.

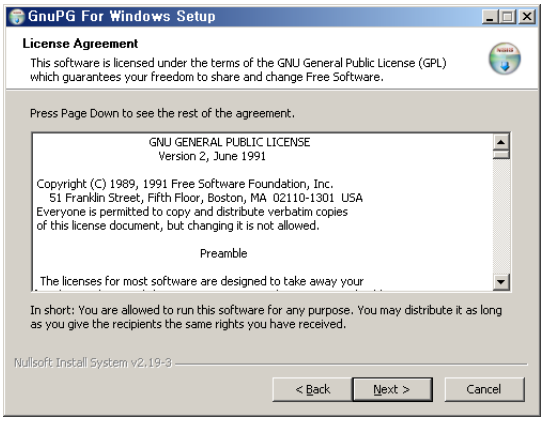
Download를 누릅니다.

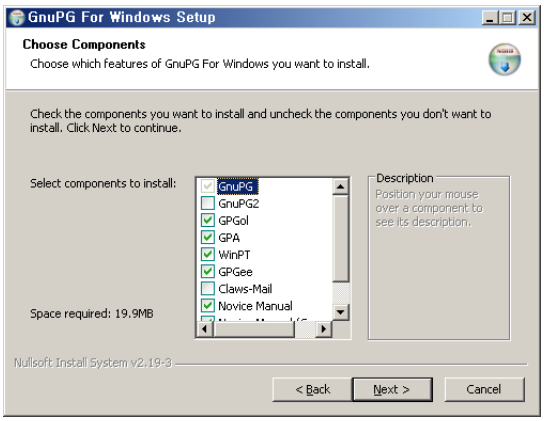


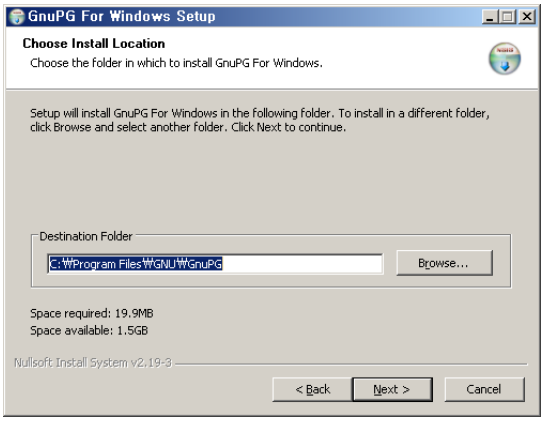
gpg4win을 누릅니다. **gpg4win light**를 누르셔도 됩니다.

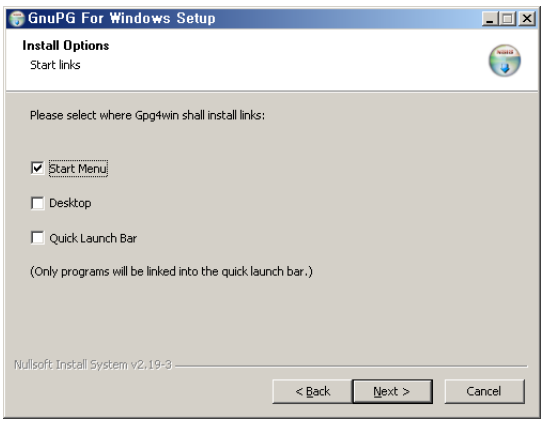
2.2 설치

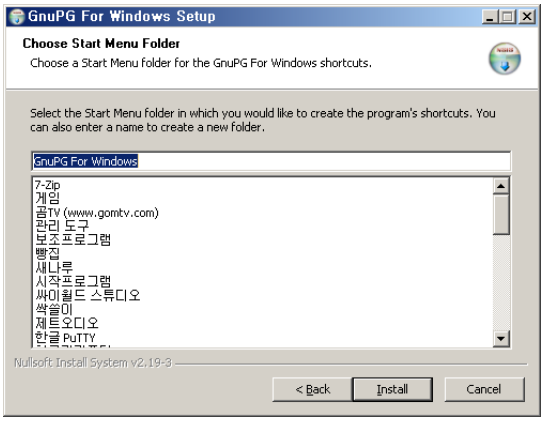
내려받은 파일을 실행하면 설치가 시작됩니다.

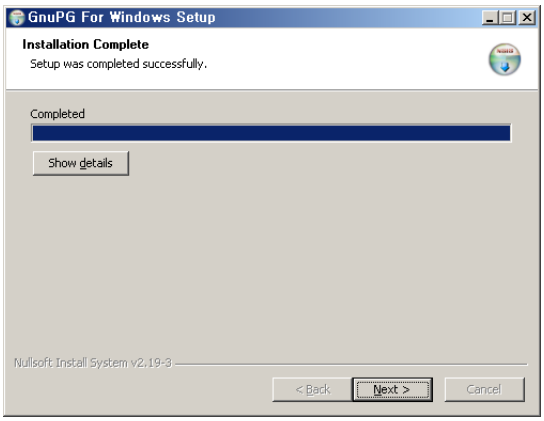

GnuPG For Windows Setup
License Agreement
This software is licensed under the terms of the GNU General Public License (GPL) which guarantees your freedom to share and change Free Software.
Press Page Down to see the rest of the agreement.
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
The licenses for most software are designed to take away your
In short: You are allowed to run this software for any purpose. You may distribute it as long as you give the recipients the same rights you have received.
Nullsoft Install System v2.19-3
< Back
Next >
Cancel


GnuPG For Windows Setup
Choose Components
Choose which features of GnuPG For Windows you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
GnuPG
GnuPG2
GPGol
GPA
WinPT
GPGee
Claws-Mail
Novice Manual
Description
Position your mouse over a component to see its description.
Space required: 19.9MB
Nullsoft Install System v2.19-3
< Back
Next >
Cancel


GnuPG For Windows Setup
Choose Install Location
Choose the folder in which to install GnuPG For Windows.
Setup will install GnuPG For Windows in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:\Program Files\GNU\GnuPG
Browse...
Space required: 19.9MB
Space available: 1.5GB
Nullsoft Install System v2.19-3
< Back
Next >
Cancel

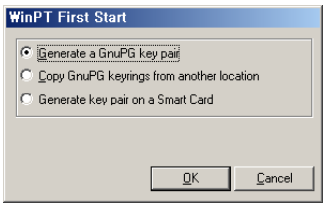

GnuPG For Windows Setup
Install Options
Start links
Please select where Gpg4win shall install links:
Start Menu
Desktop
Quick Launch Bar
(Only programs will be linked into the quick launch bar.)
Nullsoft Install System v2.19-3
< Back
Next >
Cancel





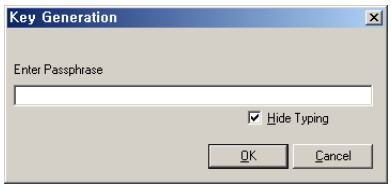
3 열쇠 만들기

설치가 끝났으면 **시작** → **프로그램** → **GnuPG For Windows** → **WinPT**를 선택합니다. 열쇠가 없으므로 다음과 같은 화면이 나옵니다.



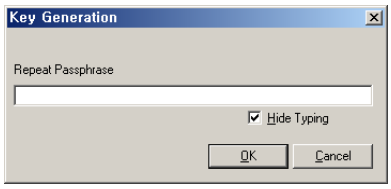
Generate a GnuPG key pair를 누르고 **OK**를 누릅니다.

이름과 이메일 주소를 입력하고 **OK**를 누릅니다.

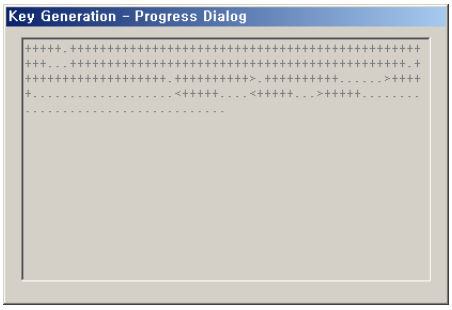


비밀문구를 입력합니다. **비밀문구**는 비밀 열쇠를 암호화할 때 쓰는 비밀번호입니다. 비밀문구는 영어로 **passphrase**라고 합니다. 비밀번호를 영어로 password라고 하는데, 충분히 길어야 한다는 것을 강조하기 위해 단어라는 뜻의 word를 어구라는 뜻의 phrase로 바꾸어서 passphrase라고 부르는 것입니다.

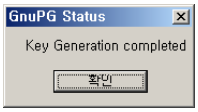
나는 기억하기 쉽지만 다른 사람은 예측하기 어려운 문장을 이용하는 것이 좋고, 중간에 특수문자를 섞는 것도 좋습니다. 영어 문장이라면 대문자와 소문자를 적절히 섞는 것이 바람직합니다.



올바로 입력했는지 확인하기 위해 한번 더 입력하면 열쇠를 만들게 됩니다.



잠시 기다리면 열쇠가 만들어집니다.



열쇠를 만들었으면 열쇠 목록에 추가하게 됩니다. 열쇠 목록을 열쇠 고리라는 뜻의 keyring이라고 부릅니다. 열쇠 목록에 추가할 때 만약에 대비하기 위해 백업을 만들 생각이 있느냐고 물어보는데, 지금은 특별히 백업할 내용이 없으므로 **아니오**를 눌러줍니다. 나중에는 백업을 위해 **예**를 누르는 것이 좋겠습니다.

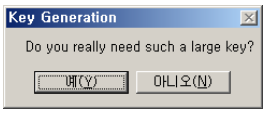
이제 트레이에 Windows Privacy Tray 아이콘이 생긴 것을 확인할 수 있습니다. 더블클릭하면 Key Manager가 실행됩니다.

3.1 열쇠 더 만들기

이메일 주소가 더 있다면 열쇠를 더 만들고 싶을 것입니다. 여기서는 방금 만든 열쇠를 지우고 새로 만들어 보겠습니다. 방금 만든 열쇠를 마우스 오른쪽 버튼으로 누르고 **Delete**를 선택하면 열쇠를 지울 수 있습니다.

이제 Key Manager의 메뉴에서 **Key** → **New** → **Expert**를 골라봅시다.

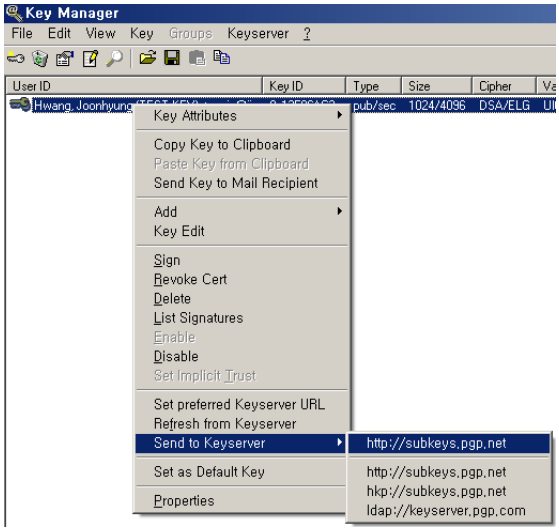
Key type은 열쇠의 종류를 말하고, Subkey size in bits는 열쇠의 크기를 말합니다. 큰 열쇠일수록 좋은 열쇠이지만, 만드는 데 시간은 오래 걸립니다. 기본값은 2048입니다. 여기서는 4096을 이용해 보도록 하겠습니다. Real name은 이름, Comment는 추가로 담고 싶은 말, Email address는 이메일 주소입니다. Expire date는 유효기간입니다. 적절한 정보를 입력한 다음, **Start**를 누릅시다.



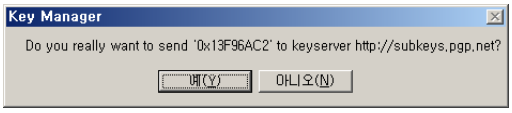
열쇠 크기를 4096으로 정해서 만드는 데 시간이 오래 걸리기 때문에 정말로 그렇게 큰 열쇠를 원하는지 물어봅니다. **예**를 선택합시다. 비밀문구를 입력하고 기다리면 열쇠가 만들어집니다. 열쇠 크기가 2048일 경우 1분 정도 걸리고, 4096일 경우 5분 이상 걸릴 수도 있습니다.

3.2 열쇠 등록하기

이제 만든 열쇠를 서버에 등록해 봅시다. 등록은 꼭 할 필요는 없지만, 등록하면 다른 사람이 쉽게 내 공개 열쇠를 받아갈 수 있습니다.



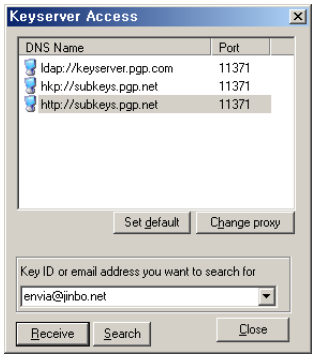
Key Manager에서 열쇠를 마우스 오른쪽 버튼으로 누르고 **Send to keyserver**를 누른 다음 아무 서버나 선택하면 됩니다. 서버들끼리 정보를 주고받기 때문에 아무 서버나 선택해도 괜찮습니다.



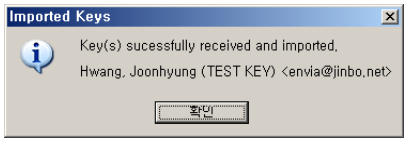
예를 누르면 열쇠가 서버에 등록됩니다.

3.3 열쇠 받아오기

이번에는 다른 사람의 공개 열쇠를 받아 봅시다. Key Manager의 메뉴에서 **Keyserver**를 선택하면 다음 화면이 나타납니다.



이메일 주소나 Key ID를 입력하면 열쇠를 받을 수 있습니다.



3.4 열쇠 내보내기

공개 열쇠를 서버에 올려 놓을 수도 있지만, 내 홈페이지에 올려 놓거나 이메일로 주고 받을 수도 있습니다. 이를 위해서는 공개 열쇠의 정보를 담은 파일을 만들어야 합니다. Key Manager에서 열쇠를 고른 다음 **Key** → **Export**를 선택하면 열쇠를 저장할 수 있습니다. 이 파일을 홈페이지에 올려 놓거나 이메일로 보내면 됩니다.

3.5 열쇠 가져오기

다른 사람의 홈페이지에서 공개 열쇠의 정보를 담은 파일을 받았거나, 이메일을 통해 받았을 경우 Key Manager에서 **Key** → **Import**를 선택한 다음 파일을 고르면 열쇠의 정보를 추가하게 됩니다.

열쇠와 fingerprint를 함께 알려 줄 경우, fingerprint를 이용해서 열쇠가 올바른 것이라는 것을 확인할 수 있습니다.

3.6 열쇠가 저장된 곳

방금 만든 열쇠들은 윈도 2000, XP의 경우 `C:\Documents and Settings\User\Application Data\gnupg`에 저장되어 있습니다. 윈도 비스타의 경우 `C:\Users\User\AppData\Roaming\gnupg`에 저장되어 있습니다. 여기에서 **User**는 윈도의 사용자 이름입니다.

3.7 주의 사항

비밀 열쇠를 잃어버릴 경우 암호화된 메일을 읽을 수 없게 됩니다. 비밀 열쇠를 실수로 지우는 일이 없도록 조심하시고, 백업해 두도록 하십시오.

비밀 열쇠를 다른 사람이 얻게 되면 암호화된 메일을 읽을 수 있게 됩니다. 비밀 열쇠를 특별한 처리 없이 저장해 놓으면 컴퓨터를 도둑맞거나 해킹을 당했을 경우 상대방은 비밀 열쇠를 얻게 되고, 암호화를 해제할 수 있습니다. 이것을 막기 위한 최후의 보루가 비밀문구입니다. 비밀 열쇠는 비밀문구로 암호화된 상태로 저장되며, 비밀 열쇠가 필요할 때마다 비밀문구를 입력받아 암호화를 해제해서 사용합니다.

비밀문구를 잊어버리면 비밀 열쇠의 암호화를 해제할 수 없으므로, 암호화된 메일을 읽을 수 없게 됩니다. 비밀문구를 잊지 않도록 주의하십시오.

비밀 열쇠와 비밀문구가 유출되지 않도록 주의하십시오.

3.8 GPGee 설정

GPGee는 파일을 암호화하고 해제하는 프로그램입니다. Gpgee에서 열쇠들을 사용할 수 있도록 설정을 해 봅시다. 아무 파일이나 마우스 오른쪽 버튼으로 누른 다음 **GPGee** → **configure**를 선택합니다.

Set program path는 보통 `C:\Program Files\GNU\GnuPG\gpg.exe`로 설정하면 됩니다. **Set options file**, **Set public keyring**, **Set secret keyring**은 위에 나와 있는 열쇠들이 들어있는 디렉터리 안을 찾아서 선택하면 됩니다. 윈도 2000, XP의 경우 보통

`C:\Documents and Settings\User\Application Data\gnupg\gpg.conf`

`C:\Documents and Settings\User\Application Data\gnupg\pubring.gpg`

`C:\Documents and Settings\User\Application Data\gnupg\secring.gpg`

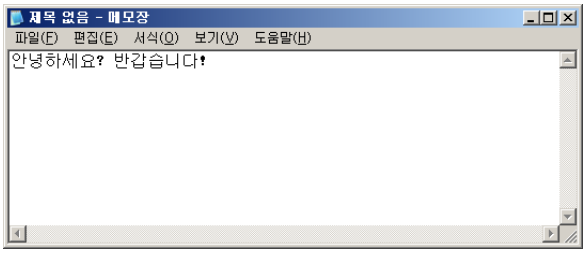
에 있습니다.

4 사용하기

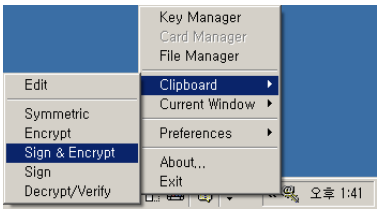
여기까지 오시느라 수고하셨습니다. 이제 암호화된 메일을 보내고 받아 봅시다.

4.1 암호화된 메일 쓰기

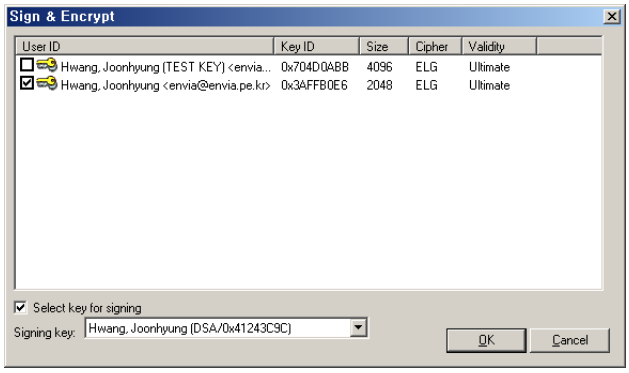
먼저 이메일의 내용을 작성합니다.



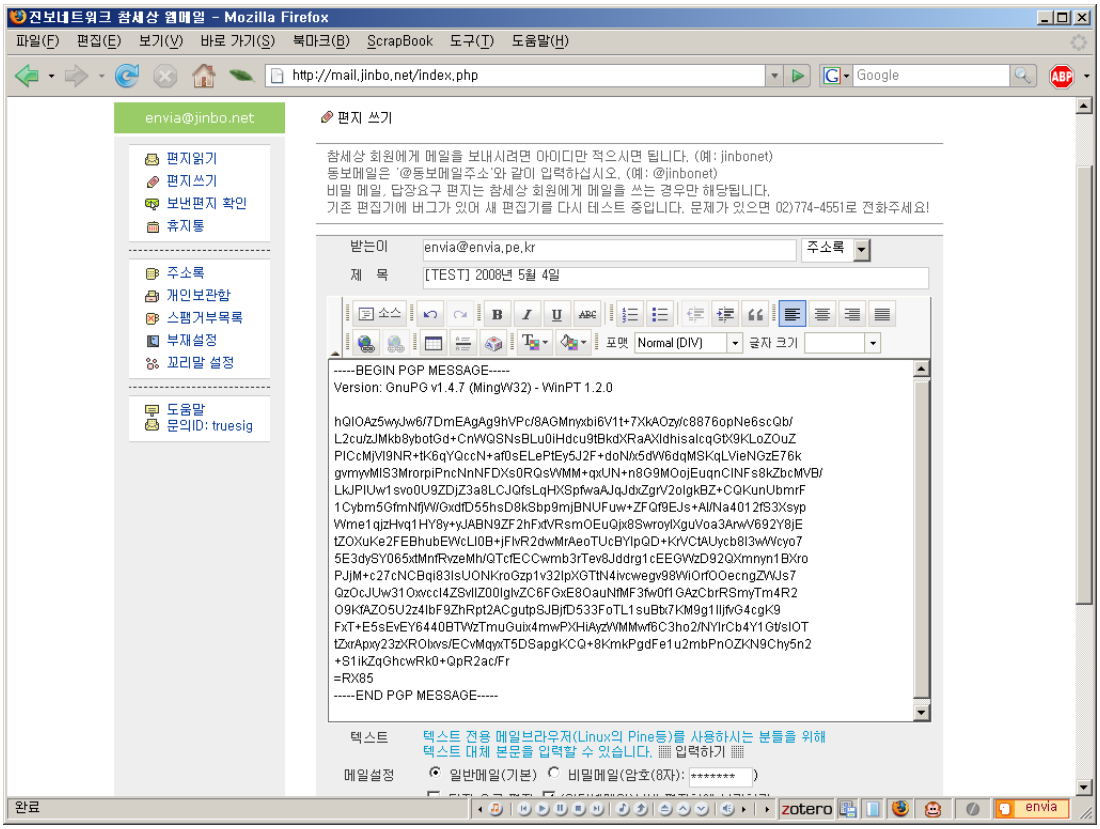
작성이 끝나면 보낼 내용 전체를 선택한 다음, 클립보드로 복사합니다. 보통 메뉴에서 **편집** → **복사**를 선택하시거나 **Ctrl+C**를 누르시면 됩니다. 그다음 트레이에 있는 아이콘을 마우스 오른쪽 버튼으로 누른 다음, **Clipboard** → **Sign & Encrypt**를 누릅니다.



열쇠를 선택합니다. 암호화에 사용할 수 있는 열쇠의 목록이 나오는데, **상대방의 열쇠**를 선택해야 합니다. 자신의 열쇠는 아래의 **Select key for signing**에서 선택해 줍니다.



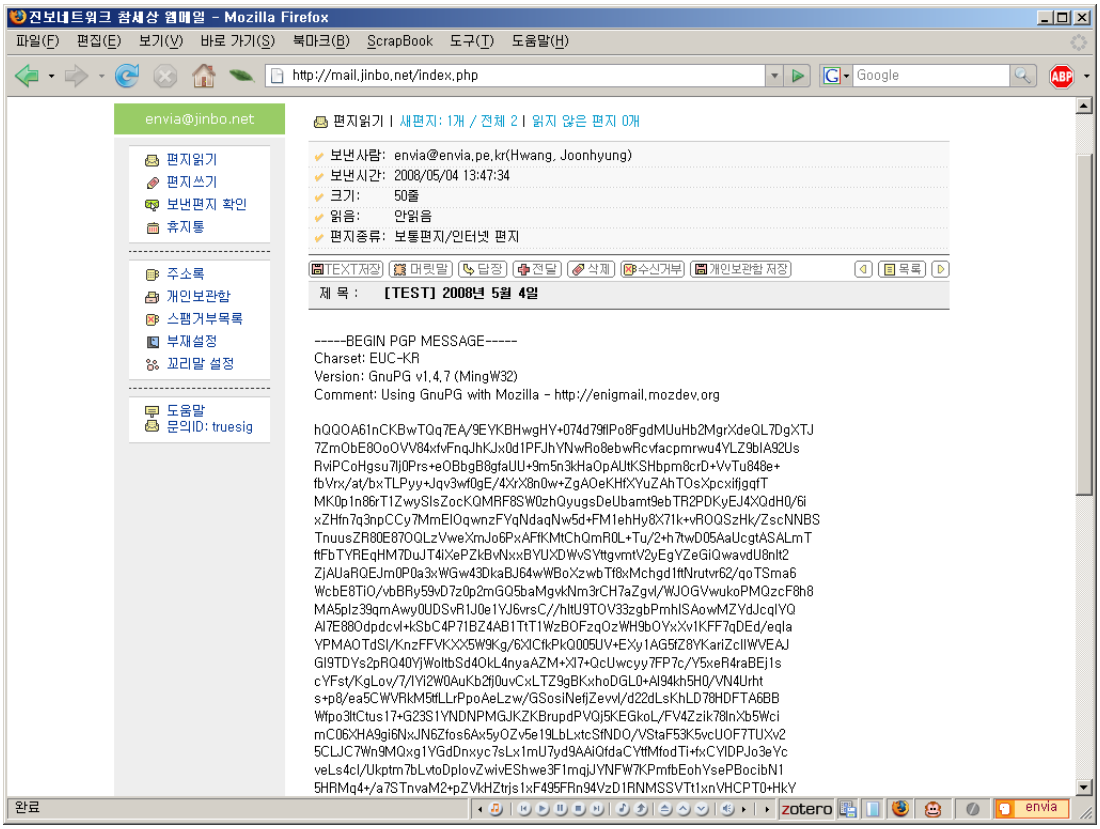
비밀문구를 입력하면 암호화가 이루어집니다. 이제 이메일을 보내는 화면에 가서 클립보드의 내용을 붙여넣으면 됩니다. **편집** → **붙여넣기**를 선택하시거나 **Ctrl+V**를 누르시면 됩니다.



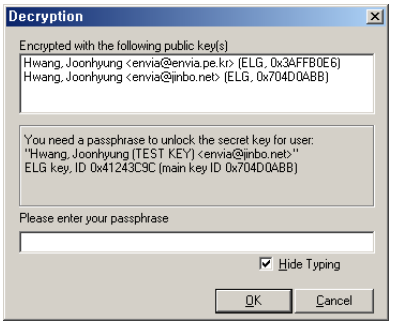
편지의 제목은 암호화 할 수 없습니다. 적절히 입력해 주시면 됩니다.

4.2 암호화된 메일 읽기

이번에는 암호화된 메일을 읽어 봅시다.



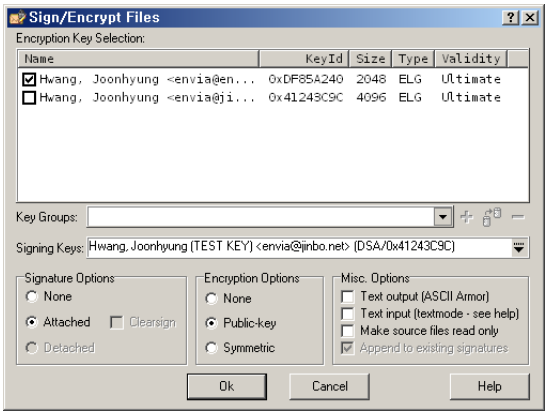
메일에서 **-----BEGIN PGP MESSAGE-----**부터 **-----END PGP MESSAGE-----**까지의 내용을 선택한 다음 클립보드로 복사합니다. 그 다음 트레이의 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **Clipboard** → **Decrypt/Verify**를 선택합니다.



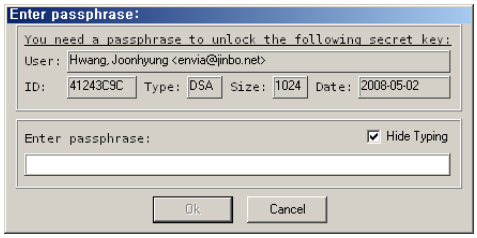
비밀문구를 입력한 후, 클립보드의 내용을 적절한 곳에 붙여넣으면 메일을 읽을 수 있습니다.

4.3 파일 암호화

암호화하고 싶은 파일을 마우스 오른쪽 버튼으로 누릅니다. 나타나는 메뉴에서 **Gpgee** → **Sign & Encrypt**를 고릅니다.



암호화에 사용하고 싶은 열쇠를 선택합니다.



비밀문구를 입력하면 암호화된 파일이 생깁니다. 암호화를 풀 때에는 마우스 오른쪽 버튼으로 누른 다음, **Gpgee** → **Verify/Decrypt**를 선택하면 됩니다.

5 참고자료

이 문서는 Use PGP with any Windows Email Client(`http://email.about.com/library/weekly/aa110199a.htm`)를 읽고 아이디어를 얻어서 작성하게 되었습니다. 다음 사이트의 내용도 도움이 되었습니다.

- GnuPG mini HOWTO (국문, `http://wiki.kldp.org/wiki.php/DocbookSgml/GnuPG-TRANS`)
- 모질라 썬더버드에서 GnuPG 사용하기 (국문, `http://docbook.kr/wiki/index.php/ThunderBird`)
- GnuPG.org (영문, `http://gnupg.org/`): GnuPG의 공식 홈페이지입니다. GnuPG와 관련된 프로그램에 대한 정보를 얻을 수 있습니다.
- Gpg4win (영문, `http://www.gpg4win.org/`): GnuPG를 윈도에서 사용할 때 필요한 프로그램들을 내려받을 수 있습니다.

암호에 관한 이론을 알고 싶으시다면 다음 책을 참고하실 수 있습니다.

- 한국정보보호학회 편, 현대 암호학 및 응용. 한국정보보호진흥원. (국문)
- Johannes Buchmann, Introduction to Cryptography, Second Edition. Springer. (영문)