IndianGNU.org - Nov,2009 - Encrypt your mails with GPG and Enigmail Thunderbird plugin

Introduction ~

GNU Privacy Guard (GnuPG or GPG) is open source/free software encryption and signing tool, alternative to the Pretty Good Privacy (**PGP**) suite of cryptographic software. **Enigmail** is an extension for Mozilla Thunderbird and other Mozilla applications. It provides public key e-mail encryption. Actual cryptographic functionality is handled by GNU Privacy Guard (GnuPG,GPG).

Step 1] Install Gnupg or GPG ?

* Ubuntu/Debian ~

root@arun:~# **apt-get install gnupg gnupg2**

* Redhat/Fedora ~

root@arun:~# **yum install gnupg gnupg2**

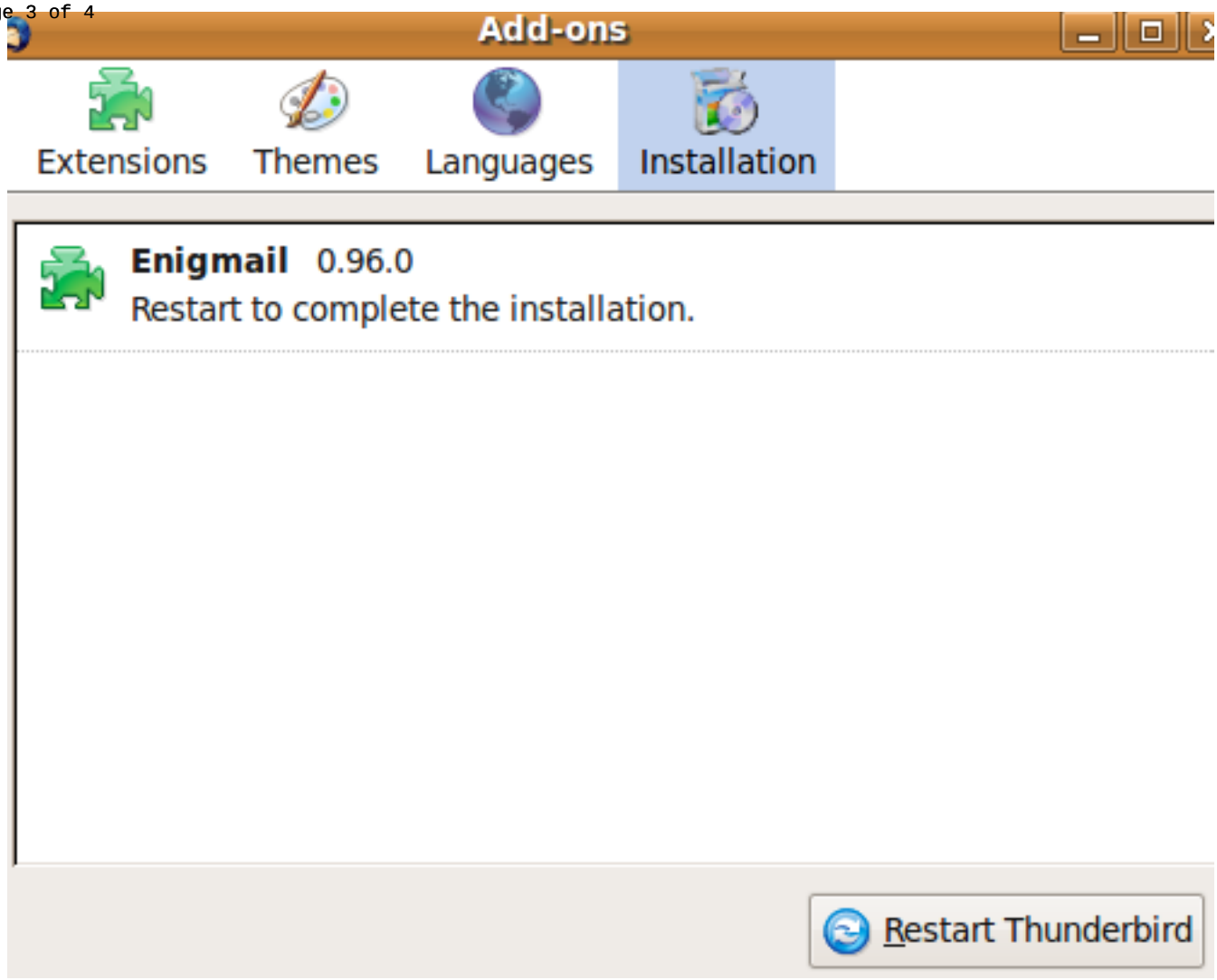
Step 2] How to Install Enigmail ?

I assume that Mozilla Thunderbird is already installed on your system. To install "Enigmail" follow following steps

a) Download "Enigmail" from url "http://enigmail.mozdev.org/download/"

Note ~ select OS and Thunderbird version properly.

b) In menu bar of the main Thunderbird window you will see **"Tools"**. Select this, and then **"Add-ons"** option. This will bring up a new window listing all of your Thunderbird plug-ins. In the lower left-hand corner of this new window you'll see a button marked "Install". Click this button. Tell Thunderbird where you saved the Enigmail .XPI file. and just say "Install" that's it!!



* Once **?Enigmail'** is installed restart the Thunderbird. Then you will see **"OpenPGP"** tab in main menu of Thunderbird.**Step 3] Setup private/public key ~**

Enigmail uses public key cryptography to ensure privacy between you and your correspondents. To generate the public/private keys, there is two methods either generate them with the help of "**gpg**" command line tool or use "enigmail"....

* We will generate private/public cryptographic keys with the help of "enigmail" as shown below....

a) Click on **"OpenPGP"** in the menu bar of the Thunderbird main window. Select "Key Management".
b) In **Enigmail** Key Manager ~ click on "Generate" tab in the menu bar and select "New key pair".
c) At the very top of the window you will see a combo box showing all of your email addresses. **GnuPG** will associate your new key with an email address.
Enigmail is just asking you which address you want to use for this key. Select whichever account will be receiving encrypted mail.

NOTE ~ We can use same keys for multiple accounts.

d) You can use passphrase or just check "No passphrase" checkbox to generate keys

without passphrase.
e) Create directory to save "Revocation Certificates"...

arunsb@arun:~$ **mkdir /home/arunsb/.gpg_key/**

f) Click on **"Generate key"** button to generate keys. done..

To share keys easily you can publish your keys with keyserver.

a) In **"Key Management"** window select your keys and then click on **?Keyserver'** tab in main menu and then click on "Upload Public Keys"
Note ~ make sure to check "Display All Keys by Default" checkbox (to list all keys)

Step 4] Compose the mail and sign it ~

Compose the mail and tell Enigmail to sign it. At the top of your Compose window you will see a button reading "OpenPGP". Click on this. Make sure that the **"Sign" option**, and only that, is checked. Finally "Send" the mail! (You will be asked for your passphrase. Once you enter it, Enigmail will sign your email and send it if you have generate keys with passphrase else it will not ask)

Enjoy!!

Regards,
Arun Bagul

Similar Posts:

- ???????? ????? ??? ??? ??? GPG ??? ???????? Enigmail Thunderbird
- ?????????? ?????? ? ??? ? Thunderbird Enigmail ???????
- GPG?Enigmail?Thunderbird??????????????????????
- Verschlüsseln Sie Ihre Mails mit GPG und Enigmail Thunderbird-Plugin
- Versleutel uw mails met GPG en Enigmail Thunderbird plugin
- Cryptez vos mails avec GPG et Enigmail plugin Thunderbird
- Mengenkripsi mail Anda dengan GPG plugin Thunderbird dan Enigmail

Be Sociable, Share!

- Tweet