PGP IMPLEMENTATION

CMP 661 Cryptography

Ali Taha Yükseldi

N18234057

1. I am going to use PGP to perform encryption. I am using Centos 7 so I will install it from "yum" repository. First I need to install the software, then generate a public/private key pair.

(base) [aty@aty ~]$ sudo yum install gnupg

[sudo] password for aty:

Loaded plugins: fastestmirror, langpacks

Determining fastest mirrors

epel/x86\_64/metalink | 27 kB 00:00:00

\* base: mirror.rackdc.com

\* epel: mirror.veriteknik.net.tr

\* extras: mirror.muvhost.com

\* nux-dextop: li.nux.ro

\* rpmfusion-free-updates: ftp-stud.hs-esslingen.de

\* updates: mirror.rackdc.com

FedoraPeople-sea | 2.9 kB 00:00:00

base | 3.6 kB 00:00:00

docker-ce-stable | 3.5 kB 00:00:00

epel | 5.3 kB 00:00:00

extras | 2.9 kB 00:00:00

nodesource | 2.5 kB 00:00:00

nux-dextop | 2.9 kB 00:00:00

rpmfusion-free-updates | 3.7 kB 00:00:01

updates | 2.9 kB 00:00:00

(1/4): rpmfusion-free-updates/x86\_64/primary\_db | 254 kB 00:00:28

(2/4): epel/x86\_64/updateinfo | 1.0 MB 00:00:45

(3/4): updates/7/x86\_64/primary\_db | 5.9 MB 00:01:53

(4/4): epel/x86\_64/primary\_db | 6.9 MB 00:02:37

Package gnupg2-2.0.22-5.el7\_5.x86\_64 already installed and latest version

Nothing to do

2. Above, it shows that GNUPG is already installed on my computer.

3. Then I will generate a public/private key pairs.

(base) [aty@aty ~]$ gpg --gen-key

gpg (GnuPG) 2.0.22; Copyright (C) 2013 Free Software Foundation, Inc.

This is free software: you are free to change and redistribute it.

There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:

(1) RSA and RSA (default)

(2) DSA and Elgamal

(3) DSA (sign only)

(4) RSA (sign only)

Your selection? RSA

Invalid selection.

Your selection? 1

RSA keys may be between 1024 and 4096 bits long.

What keysize do you want? (2048)

Requested keysize is 2048 bits

Please specify how long the key should be valid.

0 = key does not expire

<n> = key expires in n days

<n>w = key expires in n weeks

<n>m = key expires in n months

<n>y = key expires in n years

Key is valid for? (0)

Key does not expire at all

Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: aty

Name must be at least 5 characters long

Real name: alitaha

Email address: aykseldi1@yahoo.com

Comment:

You selected this USER-ID:

"alitaha <aykseldi1@yahoo.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O

You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform

some other action (type on the keyboard, move the mouse, utilize the

disks) during the prime generation; this gives the random number

generator a better chance to gain enough entropy.

We need to generate a lot of random bytes. It is a good idea to perform

some other action (type on the keyboard, move the mouse, utilize the

disks) during the prime generation; this gives the random number

generator a better chance to gain enough entropy.

gpg: key BB4F7450 marked as ultimately trusted

public and secret key created and signed.

gpg: checking the trustdb

gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model

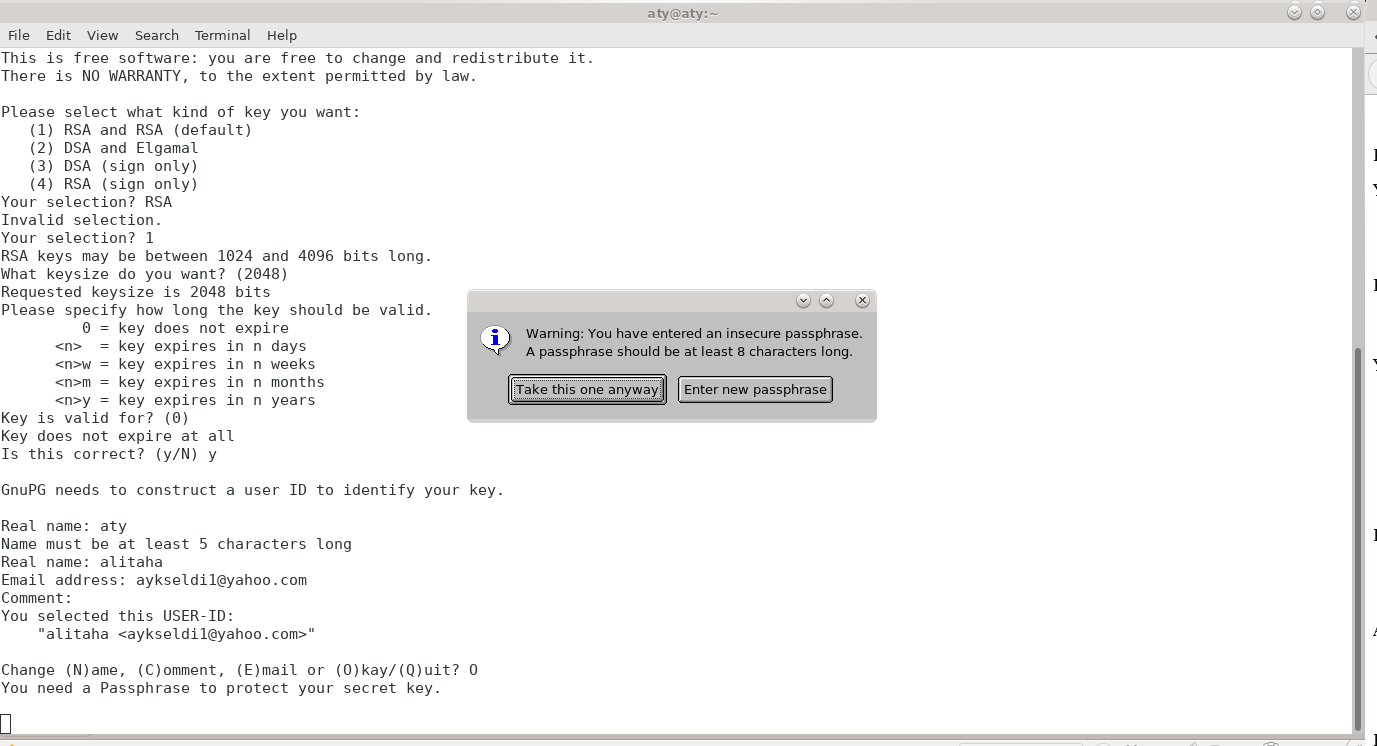
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u

pub 2048R/BB4F7450 2020-01-05

Key fingerprint = DEEA CF6B EF72 590A C711 7155 469C AA6F BB4F 7450

uid alitaha <aykseldi1@yahoo.com>

sub 2048R/1C9F094D 2020-01-05



4. I created keys and list is shown below.

(base) [aty@aty ~]$ gpg --list-keys

/home/aty/.gnupg/pubring.gpg

----------------------------

pub 2048R/BB4F7450 2020-01-05

uid alitaha <aykseldi1@yahoo.com>

sub 2048R/1C9F094D 2020-01-05

5. It's time to encrypt files with GPG. So I first created a file named plaintext.txt on /home/aty/Desktop/PGP folder. I inserted some text into file. When I run the comman , it will encrypt the file with the keys that I determined previous steps. I prefered 2048 bit RSA key pair while installation.

(base) [aty@aty PGP]$ gpg -e plaintext.txt

You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID. End with an empty line: alitaha

Current recipients:

2048R/1C9F094D 2020-01-05 "alitaha <aykseldi1@yahoo.com>"

Enter the user ID. End with an empty line:

6. I verified that I now have encrypted files present in my directory.

(base) [aty@aty PGP]$ ll

total 296

-rw-rw-r--. 1 aty aty 61 Jan 5 17:53 plaintext.txt

-rw-rw-r--. 1 aty aty 396 Jan 5 19:47 plaintext.txt.gpg

7. When I tried to view the contents of this file I found that it's a binary.

(base) [aty@aty PGP]$ cat plaintext.txt.gpg

�

��� M�&���#a��/Ŗۖ�R����

��W7�x�Q8

03��

���\_�1��-�iN��:;�W荠f����b3D

­�sq�H��bY��5�����‑�ӓ�@Xf^��z�,jD��e�<��|"��'f�(� ����\*V@�s=��/�

d\�f([��6�����m���%kX��e�ϲ��ͮ^Η�~S��3���#i�V4Jf2Q��S�n��5Ʋ\_.�y6��.ů����d��/M]�p��:�z�(s1[Cw�s�A��{h�

8W�2�E5�neXmk���q�PV�\*`��ex�=f�&�Vs��y��,dMg�]YyH;��y�t��d���F���s����������=�!I)�wL���LZ��)N��d,&;R�u

8. To decrypt a file with GnuPG/PGP, all I have to do is running gpg plaintext.txt.gpg command.

aty@aty PGP]$ gpg plaintext.txt.gpg

You need a passphrase to unlock the secret key for

user: "alitaha <aykseldi1@yahoo.com>"

2048-bit RSA key, ID 1C9F094D, created 2020-01-05 (main key ID BB4F7450)

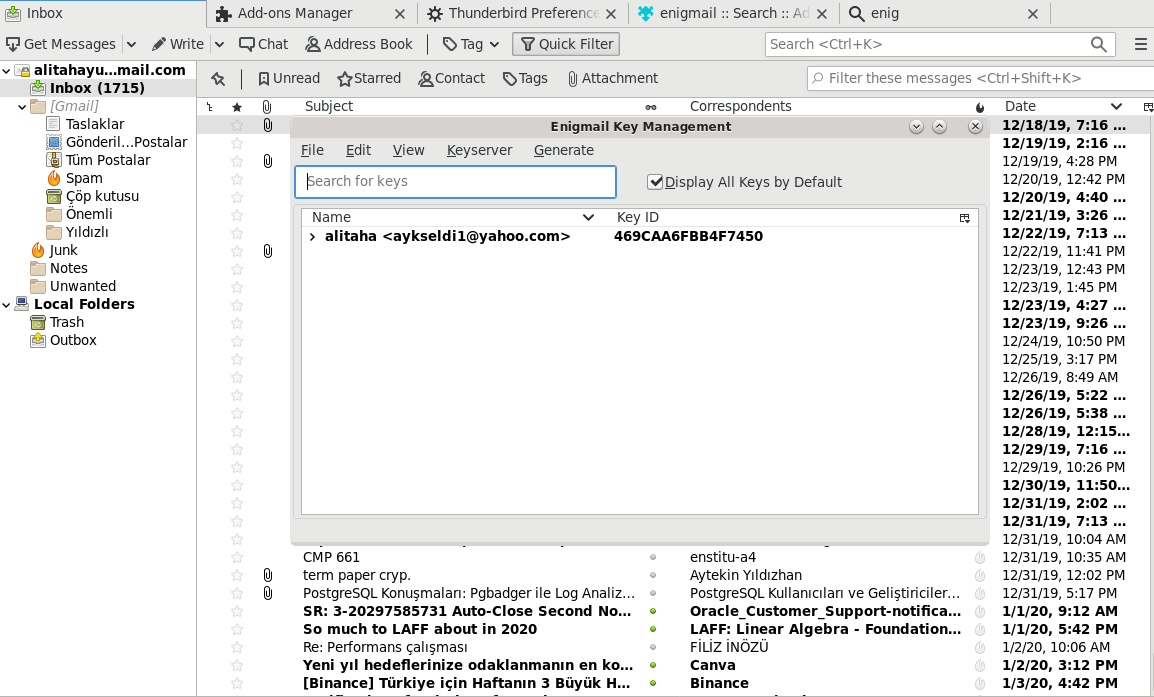
gpg: encrypted with 2048-bit RSA key, ID 1C9F094D, created 2020-01-05

"alitaha <aykseldi1@yahoo.com>"

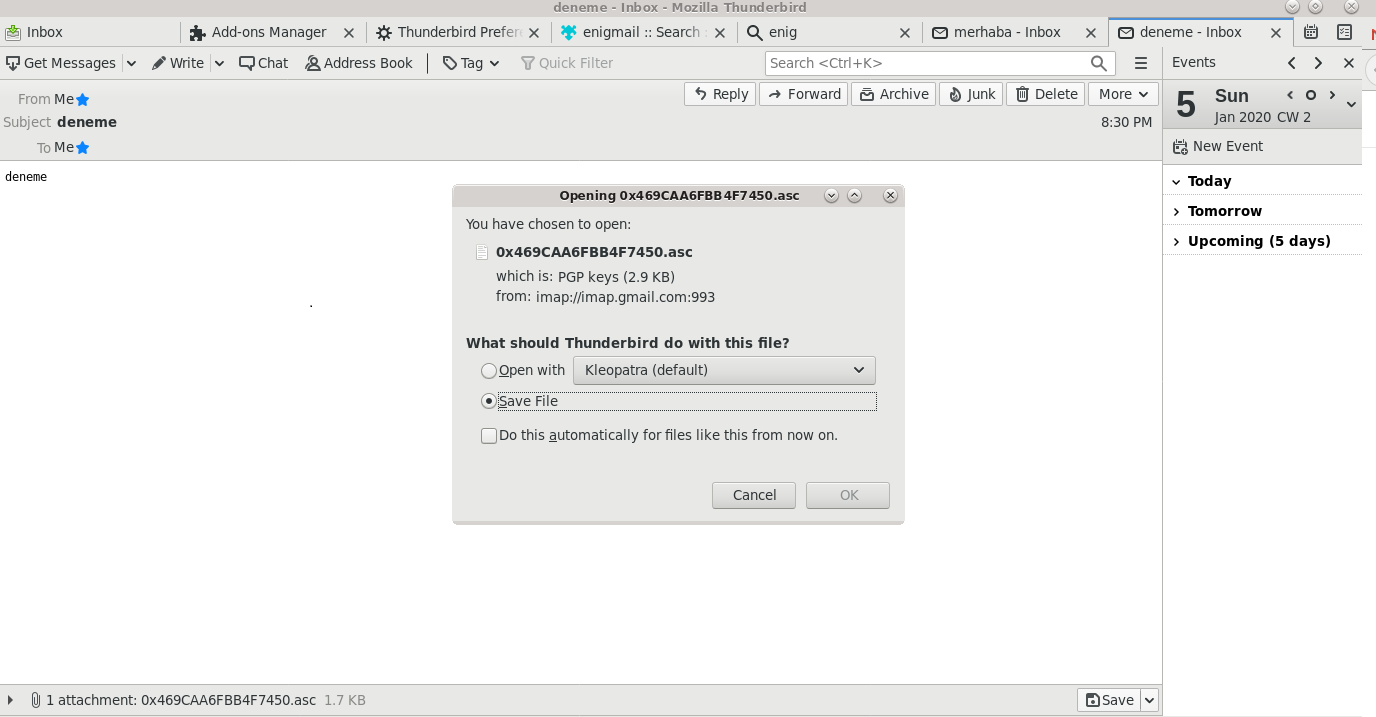
File `plaintext.txt' exists. Overwrite? (y/N) N

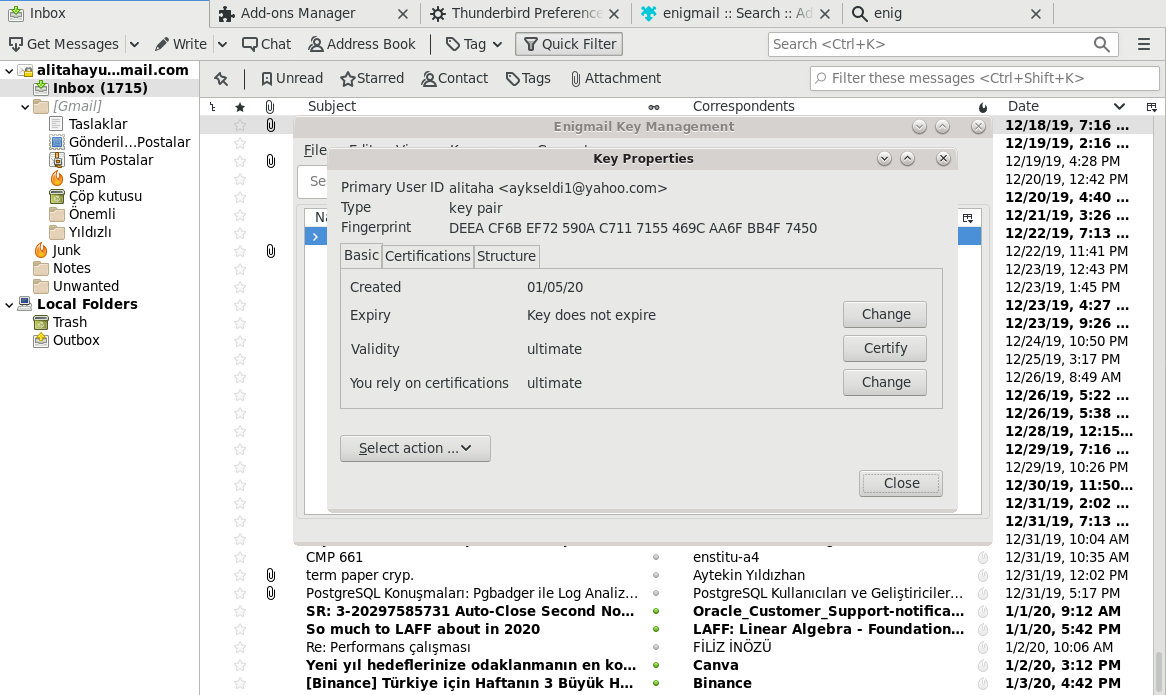
Enter new filename: plaintext\_decrypted.txt

9. I used Thunderbird as a mailer, so I need to to download and install enigmail using your Add-ons manager from Firefox. I made necessary configurations after insatllation og enigmail. Since I have already created key pairs, I just introduced them to enigmail setup.



10. At the last step, I sent a mail to another mail adress and attached my public key in it.





11. At the last step I decrypted the mail with the public key. Here is my public key, which is sent via mail to recipient.

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v2.0.22 (GNU/Linux)

mQENBF4R92YBCADyFJJBz51PPaT0YF+xT9m29rNla+Vd9Vg9Hs8YZCDOtxtZ5EvM

KW8YOaS3uCer+P5vQBGzCOMtY9poXt0GtCsYGHPtOvlWu9H2Ucpdk+ZS0atM0apZ

wMP97n65iazFk9EQGbDgqQD2Qex40Zf5k03ZJpEpNXzch93KTxp1Hq9IBK50uj5+

kD/r3+LDjGM/BsCS6cU+XdafO4Wbf9XJOekuSorXvo0KCXBx8gF9ZFN+A9XHzRdD

9FRxLETe9xcrwgXGkBFQWX7kpYSQF8J8amhp7Sub+Q5SKUAvr8hLR++UIkH6BGUv

5pdBFU2q+x5fDiQqNBg+ALNl4uQgD/SJ7yeTABEBAAG0HWFsaXRhaGEgPGF5a3Nl

bGRpMUB5YWhvby5jb20+iQE5BBMBAgAjBQJeEfdmAhsDBwsJCAcDAgEGFQgCCQoL

BBYCAwECHgECF4AACgkQRpyqb7tPdFAUaggAxLpiPWg/GY9sEmrgDv1Ld6BMqev3

QVg4eXQwiK50xRlBQH28FFDjOzzp9RWHzFfmB2nGRVtWZ0NUdyrT+pso2v2TkwqE

JXNhZbFZepOel7azFVVXQ3E5RPTcqNFnbRwpXCtf2hIX9/NVpAd4CjU+wRLXxJwW

wsouBrbhtExNzr6Qu9o86b082w+3TiGmY6ACH6REfU5GAdZmI3NQ/VadLTCOW7S+

r/jexr9pKEuX0kUzerf8/0hdXBDV4Kn4ZZlWNF5c/bbMZMyJ2AYd9TQBPzH7pVMt

MWbwgrPW/4hWYNSscV6N19RUDUqLFB+sGUPrXqZYq0LgpVaGIgmNtTF3CLkBDQRe

EfdmAQgAs7JqQOFNJgzoDsparaOLSm2VmnEYT9je0IQjT1ZqSZpSruSEsC2mjnPW

DLDEnLv2uVCwiyRsBJG6Vv1xtJaMPyi+xMga1mg5boRiWVzV61LnHJK9Y/7ynFx7

uKYoyLv55HNy77Emwhk1iuJ2621haQmYT1R4aQladhRuxQ9ngNEAHcZ8h9fWJmMA

JTHcttPWGtdqKYYBTB/9tKa9qTV19In3CgoSBOUPmCiswr3vQ8B1Zi6JGnQ/kGfS

kLf8piwfyZJvEMduDT8qtP0k0z2dAcovddnOPBExOoSeqlk+5ReOGppd6E6zWMtq

s6auVzg5m71g6To8pY8fy2Pn4JG59QARAQABiQEfBBgBAgAJBQJeEfdmAhsMAAoJ

EEacqm+7T3RQMJQIAN3pGaO0efCg9Ml1d4zAnl76nb15N9LKM7Lks2GUlHWI1TVz

H1u8QoH0lVuDQypqPCAF/Nt2l8jAfGfkhDRvLtw1RUWMul0ewtZkbTPh8spPS/w7

8KngmXhv+CvQXarKIF96lNFV9WstFC9BNc3xIuHFe5c2roC4217dK3mPrcyiMD25

wcVsqbyeNH39s2upPQCPeHQ7mIdW7MopHCFwwTHHiGCQCKR4K2+6aHgpZ3YoIkMf

khZTGabRaYSWUMucmRiLr392l0S6Mlb1fSa6Hq6CXoAqv18B1a+ot7ohTya0/Rod

eCoE/ZBUVDC/rJDpOC3/vT5jmQzunyaUhVQJ9jk=

=ruME

-----END PGP PUBLIC KEY BLOCK-----