# Praktikum Kriptografi

## Implementasi GnuPG pada Linux

Pada praktikum ini diasumsikan user dudi akan mengirimkan sebuah file ke user badu.

### Lab 1. Membuat gpg keypair

Untuk menerapkan kriptografi menggunakan gpg, Anda harus membuat dahulu gpg keypair (pasangan private dan public key). Caranya sebagai berikut:

```
dudi@ubuntu:~$ gpg --gen-key
gpg (GnuPG) 2.2.4; Copyright (C) 2017 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.

Note: Use "gpg --full-generate-key" for a full featured key generation
dialog.

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

Real name: Dudi Fitriahadi
Email address: dudi.fitriahadi@gmail.com
You selected this USER-ID:
    "Dudi Fitriahadi <dudi.fitriahadi@gmail.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o
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 FB2E3BD842429013 marked as ultimately trusted
gpg: directory '/home/dudi/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/dudi/.gnupg/openpgp-
revocs.d/DA1D378C864E28B80DF27756FB2E3BD842429013.rev'
public and secret key created and signed.

pub   rsa3072 2020-02-06 [SC] [expires: 2022-02-05]
      DA1D378C864E28B80DF27756FB2E3BD842429013
uid                      Dudi Fitriahadi <dudi.fitriahadi@gmail.com>
sub   rsa3072 2020-02-06 [E] [expires: 2022-02-05]
dudi@ubuntu:~$
```

### Lab 2. Menampilkan daftar keys

- Menampilkan daftar private key:

```
dudi@ubuntu:~$ gpg --list-secret-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2022-02-05
/home/dudi/.gnupg/pubring.kbx
```

```
------------------------------
sec   rsa3072 2020-02-06 [SC] [expires: 2022-02-05]
      DA1D378C864E28B80DF27756FB2E3BD842429013
uid           [ultimate] Dudi Fitriahadi <dudi.fitriahadi@gmail.com>
ssb   rsa3072 2020-02-06 [E] [expires: 2022-02-05]
dudi@ubuntu:~$
```

- Menampilkan daftar public key:

```
dudi@ubuntu:~$ gpg --list-public-keys
/home/dudi/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2020-02-06 [SC] [expires: 2022-02-05]
      DA1D378C864E28B80DF27756FB2E3BD842429013
uid           [ultimate] Dudi Fitriahadi <dudi.fitriahadi@gmail.com>
sub   rsa3072 2020-02-06 [E] [expires: 2022-02-05]
dudi@ubuntu:~$
```

**Lab 3. Mengekspor public key untuk diberikan kepada teman anda**

- Untuk mengekspor public key anda gunakan perintah berikut:

```
dudi@ubuntu:~$ gpg -a -o dudi.key --export dudi.fitriahadi@gmail.com
dudi@ubuntu:~$ ls -l dudi.key
-rw-r--r-- 1 dudi dudi 2468 Feb  7 01:29 dudi.key
dudi@ubuntu:~$
```

- Selanjutnya file dudi.key tersebut dapat diberikan ke teman-teman Anda

**Lab 4. Menambahkan public key milik teman anda ke dalam daftar keys**

- Untuk mengimpor public key milik teman anda gunakan perintah berikut:

```
badu@ubuntu:~$ ls -l dudi.key
-rw-r--r-- 1 badu badu 2468 Feb  7 01:50 dudi.key
badu@ubuntu:~$ gpg --import dudi.key
gpg: key FB2E3BD842429013: public key "Dudi Fitriahadi
<dudi.fitriahadi@gmail.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
badu@ubuntu:~$
```

- Kemudian periksa daftar public key:

```
badu@ubuntu:~$ gpg --list-public-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2022-02-05
/home/badu/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2020-02-06 [SC] [expires: 2022-02-05]
      B4B01EC54D0B0090661474FDC318C4D60F36CA69
uid           [ultimate] Badu Raharjo <badu.raharjo@gmail.com>
sub   rsa3072 2020-02-06 [E] [expires: 2022-02-05]
```

```
pub   rsa3072 2020-02-06 [SC] [expires: 2022-02-05]
      DA1D378C864E28B80DF27756FB2E3BD842429013
uid           [ unknown] Dudi Fitriahadi <dudi.fitriahadi@gmail.com>
sub   rsa3072 2020-02-06 [E] [expires: 2022-02-05]
badu@ubuntu:~$
```

**Lab 5. Mengenkripsi File yang akan diberikan kepada teman anda**

- Agar file yang akan anda berikan tidak dapat dibuka oleh orang yang tidak berhak, ada baiknya file tersebut dienkripsi sebelum dikirimkan dengan cara sbb:

```
dudi@ubuntu:~$ ls -l coba.txt
-rw-r--r-- 1 dudi dudi 27 Feb  7 01:43 coba.txt
dudi@dudi-Aspire:~$ cat coba.txt
echo Hallo
echo Apa kabar?
dudi@ubuntu:~$ gpg -e -r badu.raharjo@gmail.com coba.txt
gpg: B6A347AB4125903C: There is no assurance this key belongs to the
named user
sub  rsa3072/B6A347AB4125903C 2020-02-06 Badu Raharjo
<badu.raharjo@gmail.com>
 Primary key fingerprint: B4B0 1EC5 4D0B 0090 6614  74FD C318 C4D6
0F36 CA69
      Subkey fingerprint: 247A 610A 33BF 09A1 F9BB  D382 B6A3 47AB
4125 903C

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
dudi@ubuntu:~$
```

- Hasil perintah enkripsi di atas adalah file coba.txt.gpg yang merupakan file dengan format binari. Periksa dengan perintah berikut:

```
dudi@ubuntu:~$ ls -l coba.txt*
-rw-r--r-- 1 dudi dudi  27 Feb  7 01:43 coba.txt
-rw-r--r-- 1 dudi dudi 492 Feb  7 01:44 coba.txt.gpg
dudi@ubuntu:~$ cat coba.txt
echo Hallo
echo Apa kabar?
dudi@ubuntu:~$ cat coba.txt.gpg
[illegible]
                                        [illegible]
[illegible]
[illegible]
[illegible]

hd[illegible]
[illegible]
```

```
##HK@#Bi'@@#@J@'ns@@K#_9@@6ς#@=n#DX@cnY@#@Me@#W@=-
@@@@ч#H@2"Y7@=@@$#@@)@@@@@[E[#g@@#@#@@@M @u@H@@#@@&@u@Ḃ
                                        7@@djB@@@@@@@@@#@rm[7#@ϰ@k⌊F@@ᵞ@@@.@@
%#]@@@[#M#@>@F@@
@9@@@A%@@R#<@i@@7@@=#@@@f#@@k0@@5⌊@ t-@##@|t@#@
                                                                7Z #9@E@攵@@(@
  _e#)@#dudi@ubuntu:~$
```

**Lab 6. Mendekripsi File dari teman anda**

- Agar file terenkripsi yang anda terima dari teman anda dapat dibaca maka harus didekripsi terlebih dahulu dengan menggunakan perintah berikut:

```
badu@ubuntu:~$ gpg -d -o hasil.txt coba.txt.gpg
gpg: encrypted with 3072-bit RSA key, ID B6A347AB4125903C, created
2020-02-06
      "Badu Raharjo <badu.raharjo@gmail.com>"
badu@ubuntu:~$ ls -l hasil.txt
-rw-r--r-- 1 badu badu 27 Feb  7 02:03 hasil.txt
badu@ubuntu:~$ cat hasil.txt
echo Hallo
echo Apa kabar?
badu@ubuntu:~$
```

**Lab 7. Menandatangani File Text**

- Untuk menjamin bahwa file yang akan Anda berikan kepada teman Anda adalah file yang sah berasal dari Anda, dapat dilakukan dengan menandatangani file tersebut. Caranya sebagai berikut:

```
dudi@ubuntu:~$ gpg --clearsign coba.txt
```

- Hasilnya adalah file coba.txt.asc (lihat terdapat tanda tangan digital di baris bawah dari file coba.txt.asc)

```
dudi@ubuntu:~$ ls -l coba*
-rw-r--r-- 1 dudi dudi  27 Feb  7 01:43 coba.txt
-rw-r--r-- 1 dudi dudi 735 Feb  7 02:17 coba.txt.asc
-rw-r--r-- 1 dudi dudi 492 Feb  7 02:05 coba.txt.gpg
dudi@ubuntu:~$ cat coba.txt.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

echo Hallo
echo Apa kabar?
-----BEGIN PGP SIGNATURE-----

iQGzBAEBCgAdFiEE2h03jIZOKLgN8ndW+y472EJCkBMFAl48ZlgACgkQ+y472EJC
kBOKpwv+KWB+k4RWcv5JWZyXPLgoTXo5T7oSDKffuPj+7JSyfDuDB1AmSsmuVgaa
u6HxTnlDL6dZqCmu3O7bMYgzkdcenFKLsFsGFPCLbwjuvTXh8a11aLbZC9CgBr4F
KZa5eLnN0cljsMSw2NkhB5f7Ii0wA2HXhjTnmS+jgHnx+a32tYrFy3hJ76geLNZX
y8kiuOD3X1ykWqEvnQOX3NQzJHui+YDfplc7FNvIJwZ6lv65LOsbt+TCCEfVrecP
94ZsJP1YVPC3m5P22h07DxiyXQzpE12Pdp20GrY+VmqZzN7JtimHFXyUBx1jO0VP
```

```
X82Fxjez4LJlqX6IJwlkYdKYj/bHcX1o3IPcxOjW+v/ld3sLSlv1FZZ/vk7v/Xy/
l5YwRHbi0B8gptlBLCzNNTIWN2HUiMw9eb+t2snlpTWhH0Mp6hZFnibgFGGDw+5z
Dmg6SzjCCZM6BIf6Qn66ZzkEItBHpM2bXgR1s59BWVMjb69XLz14yjZiQVxQ/22h
MKQCdPyk
=ero6
-----END PGP SIGNATURE-----
dudi@ubuntu:~$
```

### Lab 8. Memverifikasi tanda tangan digital

- File yang bertanda tangan digital yang telah diperoleh dari teman dapat Anda verifikasi kebenarannya dengan perintah berikut:

```
badu@ubuntu:~$ gpg --verify coba.txt.asc
gpg: Signature made Jum 07 Feb 2020 02:17:44  WIB
gpg:                using RSA key DA1D378C864E28B80DF27756FB2E3BD842429013
gpg: Good signature from "Dudi Fitriahadi <dudi.fitriahadi@gmail.com>"
[unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: DA1D 378C 864E 28B8 0DF2  7756 FB2E 3BD8 4242 9013
gpg: WARNING: not a detached signature; file 'coba.txt' was NOT verified!
badu@ubuntu:~$
```