GNU Privacy Guard (GPG) Cheatsheet

GnuPG adalah implementasi lengkap dan bersifat gratis untuk standar enkripsi OpenPGP yang dijelaskan menurut RFC4880 (dikenal juga sebagai PGP). GnuPG memberikan kemampuan untuk enkripsi dan penandatanganan digital data untuk pertukaran data antar perangkat. GnuPG dilengkapi dengan key management system yang baik, dan akses ke beragam direktori public key. GnuPG atau GPG merupakan aplikasi berbentuk command line dengan fitur lengkap untuk integrasi dengan aplikasi enkripsi yang lainnya.

PEMASANGAN APLIKASI GNUPG

Aplikasi GPG tersedia di platform Linux, MacOS, dan Windows, yang dapat diunduh di :
https://www.gnupg.org/

BANTUAN

Menampilkan daftar perintah dan bantuan untuk operasi GPG

```
gpg --help
```

PEMBUATAN KEY PAIRS

Membuat pasangan key pair untuk private key dan public key.

```
gpg --gen-key
gpg --expert --full-generate-key
```

PEMBUATAN REVOKE KEY

Membuat key untuk pembatalan sertifikat dari private key dan public key.

```
gpg -v -a -o [nama file output] <spasi>
--generate-revocation [UID]
```

DAFTAR PUBLIC KEY GPG

Lihat daftar key pair publik yang telah dibuat dan disimpan ke dalam aplikasi GPG.

```
gpg --list-keys
gpg --list-sigs
```

DAFTAR PRIVATE KEY GPG

Lihat daftar private key pair yang disimpan di dalam aplikasi GPG.

```
gpg --list-secret-keys
```

HAPUS KEY PAIR TERSIMPAN

Menghapus key pair public key dan private key dari daftar penyimpanan GPG. Dimulai dari menghapus private key terlebih dahulu lalu diikuti menghapus public key.

```
gpg --delete-secret-key [UID]
gpg --delete-key [UID]
```

HAPUS PUBLIC KEY PAIR

Jika ingin menghapus public key pair milik pengguna GPG lain, cukup jalankan.

```
gpg --delete-key [UID]
```

EKSPOR PUBLIC KEY PAIR

Melakukan ekspor public key dengan pengaman kode ASCII dan dijadikan dalam bentuk file data.

```
Gpg -v -a -o publickey.asc --export [UID]
```

EKSPOR PRIVATE KEY PAIR

Melakukan ekspor private key dengan pengaman kode ASCII dan dijadikan dalam bentuk data.

```
gpg -v -a -o  privatekey.asc --export-secret-key
[UID]
```

EKSPOR SUB KEY PAIR

Ekspor key pair subkey dari private key .

```
gpg -v -a -o secretsubkey.asc --export-secret-
subkeys [UID]
```

IMPOR KEY PAIR

Melakukan impor data key value pair berupa secret key atau public key.

```
gpg --import [nama file atau path ke file
key pair]
```

EDIT DATA KEY PAIR

Mengubah data-data yang tersimpan dalam key value pair untuk private key.

```
gpg --expert --edit-key [UID]
```

ENKRIPSI DATA

Enkripsi data dengan pengaman kode ASCII, lalu berikan tanda tangan digital pengaman dengan kunci public key penerima data, dan jadikan ke bentuk file teks atau file ASCII.

```
gpg -a -s -e -u [UID private key] -r [UID
public key penerima data] -o [nama output
file] [file yang akan dikenkripsi]
```

Contoh : Enkripsi data bernama filepenting.txt dan amankan dengan public key milik penerima kiriman data. File dienkripsi menjadi bentuk .txt yang baru.

```
gpg -a -s -e -u kucingpembuat -r
kucingpenerima -o
filepentingenkrip.txt.asc filepenting.txt
```

ENKRIPSI DENGAN ALGORITMA KHUSUS

Menggunakan algoritma kustomisasi untuk enkripsi data.

```
gpg -a -s -e --cipher-algo [tipe
algoritma] -r [UID public key penerima
data] -o [nama output file] [file yang
akan dikenkripsi]
```

Contoh dengan enkripsi AES256 :

```
gpg -a -s -e --cipher-algo aes256 -r
kucingpenerima -o
filepentingenkrip.txt.asc filepenting.txt
```

ENKRIPSI DENGAN SECRET KEY PILIHAN

Enkripsi data dengan secret key tertentu jika di dalam keyring GPG terdapat banyak secret key . Tambahkan tag **-u** atau --**local-user** untuk memilih secret key pilihan.

```
Gpg -v -a -s -e -u [UID secret key] -r [UID public key penerima data] -o [nama output file] [file yang akan dikenkripsi]
```

Contoh :

```
gpg -v -a -s -e -u myUID -r penerimaUID -o outputfile.doc.asc inputfile.doc
```

MEMBUAT SIGNATURE FILE ENKRIPSI

Membuat tanda tangan signature untuk verifikasi data yang dienkripsi

```
gpg -a -u [UID private key] -r [UID public key] -o [namafile_signature.sig] --detach-sig [namafile_terenkripsi]
```

Contoh :

```
gpg -a -u kucingprivate -r penerimapublic -o filepentingenkrip.sig --detach-sig filepentingenkrip.txt
```

VERIFIKASI DATA DENGAN SIGNATURE

Melakukan verifikasi data yang dienkripsi dengan menggunakan file signature yang disertakan.

```
gpg --verify [nama atau path ke file signature] [nama dokumen yang terenkripsi]
```

Contoh :

```
gpg --verify filepentingenkrip.sig filepentingenkrip.txt
```

DEKRIPSI DATA TERENKRIPSI

Mengembalikan kembali data yang telah dienkripsi menjadi bentuk data aslinya.

```
gpg -d -o [file_output] [file_enkripsi]
```

Contoh:

```
gpg -d -o filepenting.txt <spasi> fileterenkrip.txt.asc
```

EKSPOR PUBLIC KEY KE KEYSERVER

Kirim public key ke layanan keyserver online untuk distribusi ke banyak pengguna.

```
gpg --keyserver [alamat server keyserver] -send-keys [public key ID atau UID]
```

IMPOR PUBLIC KEY DARI KEYSERVER

Ambil data public key dari keyserver tertentu dan dengan public key ID tertentu.

```
gpg --keyserver [alamat server keyserver] --receive-keys [public key ID]
```

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

PERTUKARAN DATA DUA PENGGUNA

Ada dua pengguna yang ingin bertukar data yang dienkripsi dengan GPG. Sebut saja pengguna A dan Pengguna B. Keduanya akan mengirim data yang dienkripsi dengan public key dan secret key masing-masing. Kemudian melakukan proses dekripsi untuk mengembalikan data file terenkripsi.

Langkah 1 . Pengguna A membuat private key dan *public key, lalu public key ini diberi nama publickey_penggunaA.asc* . Pengguna B juga melakukan langkah yang sama, dan membuat public key yang diberi nama *publickey_penggunaB.asc* . Keduanya lalu saling bertukar public key dan melakukan penambahan impor public key ke masing-masing keyring GPG.

Langkah 2 . Pengguna A ingin mengirim data ke pengguna B dengan data yang dienkripsi. Data yang akan dikirim berbentuk *dokumenpenting.doc* . Pengguna A melakukan enkripsi dan penandatanganan data dengan public key dari pengguna B, dengan perintah *gpg -a -s -e -r [uid_penggunaB] -o [dokumenpenting_encrypt.asc] [dokumenpenting.doc]* . Hasil enkripsi data ini bernama *dokumenpenting_encrypt.asc* . Pengguna A juga dapat menambahkan signature dari dokumen yang telah dienkripsi dan diberi nama *dokumenpenting_encrypt.asc.sig* . Data yang telah dienkripsi dan signature nya lalu dikirim ke pengguna B melalui media ataupun saluran elekronik lainnya.

Langkah 3 . Pengguna B menerima kiriman data dari pengguna A yang berupa *dokumenpenting_encrypt.asc* dan *dokumenpenting_encrypt.asc.sig* . Pengguna B bisa melakukan verifikasi data dengan signature yang disertakan.

Langkah 4 . Pengguna B lalu melakukan **decrypt** data yang diterima untuk mengembalikan data ke bentuk semula, yaitu *dokumenpenting.doc*. Pengguna B dapat juga mengirim data ke pengguna A dengan langkah yang sama. Namun bedanya adalah pengguna B melakukan enkripsi dan tanda tangan data dengan public key milik pengguna A.

TIPS

1. Setelah membuat key pair private key dan public key, segera lakukan pembuatan revoke key.
3. Ekspor private key , public key, dan revoke key ke bentuk file berekstensi .txt atau .asc . Kemudian lakukan backup ke media fisik seperti USB Drive, CD, DVD. Simpan di tempat yang aman dan tersegel.
4. Setelah melakukan backup, hapus private key dan public key setelah tidak digunakan untuk melakukan enkripsi data dan dekripsi data. Impor kembali private key dan public key jika dibutuhkan kembali untuk proses enkripsi dan dekripsi.
5. Lakukan proses pemampatan atau compressing pada data yang akan dienkripsi. Misalnya kompres data menjadi berbentuk .zip atau .tar.gz atau .rar .
6. Tips lebih lanjut dapat dilihat pada artikel Medium bahasa Indonesia berikut ini.

http://bit.ly/KunciRahasiaGPG

disusun oleh kucingmumu@kucing.io