KEAMANAN SISTEM DAN JARINGAN
ENKRIPSI DAN HASHING

RINANZA ZULMY ALHAMRI, S.Kom., M.Kom
PSDKU POLINEMA DI KOTA KEDIRI

Kode : KIF195004
Kredit : 3 SKS
Semester : 5

MENU

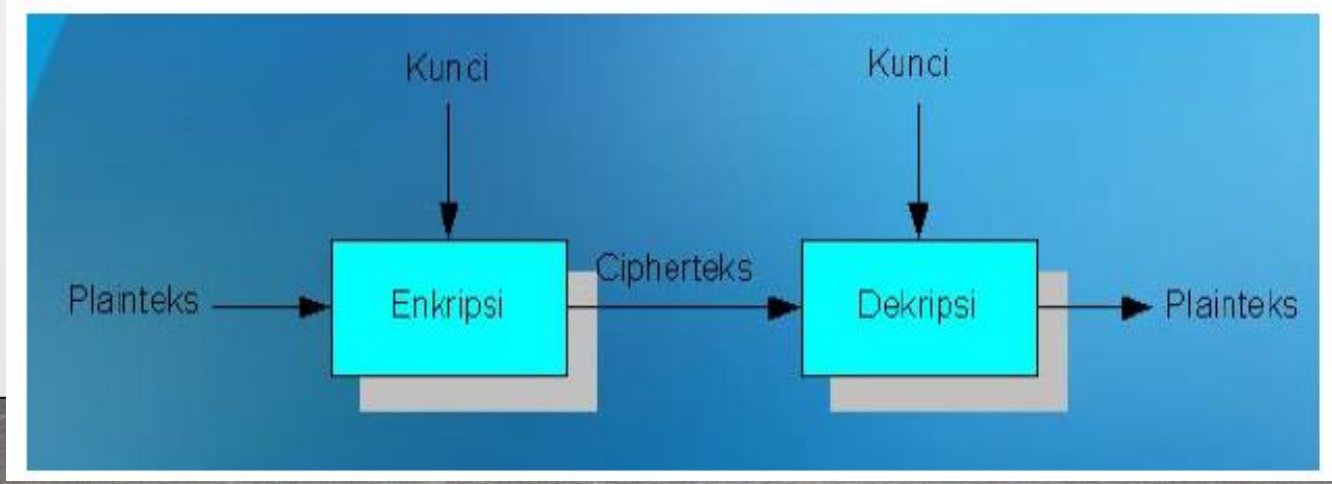
- Konsep Kriptografi
- Konsep Enkripsi/Dekripsi
- Konsep Hashing
- Enkripsi Simetris Menggunakan GPG
- Enkripsi Asimetris Menggunakan GPG
- Hashing Menggunakan Checksum
- Tugas

Konsep Kriptografi

- **Kriptografi** (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. "*Crypto*" berarti "*secret*" (rahasia) dan "*graphy*" berarti "*writing*" (tulisan)
- **Algoritma Kriptografik** (*cryptographic algorithm*), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi.
- Kriptologi (cryptology): studi mengenai kriptografi dan kriptanalisis
- Persamaan kriptografer dan kriptanalis:
  - Keduanya sama-sama menerjemahkan cipherteks menjadi plainteks
- Perbedaan kriptografer dan kriptanalis:
  - Kriptografer bekerja atas legitimasi pengirim atau penerima pesan
  - Kriptanalis bekerja tanpa legitimasi pengirim atau penerima pesan

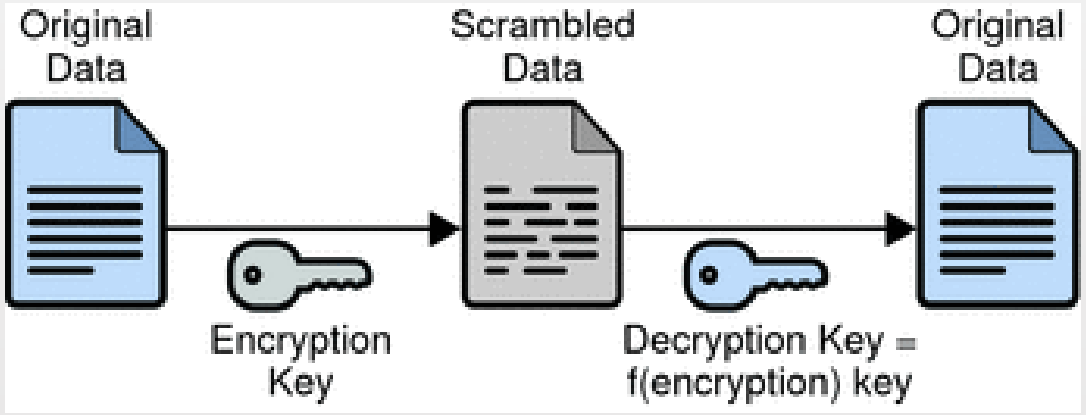
Konsep Enkripsi/Dekripsi

- **Enkripsi** *(encryption)* merupkan proses yang dilakukan untuk mengamankan sebuah pesan (*plaintext*) menjadi pesan yang tersembunyi (*ciphertext*)
- ***Ciphertext*** adalah pesan yang sudah tidak dapat dibaca dengan mudah.
- **Dekripsi** (*decryption*) merupakan proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*.
- Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak.
- Dengan enkripsi data disandikan (encrypted) dengan menggunakan sebuah kunci (key).
- Untuk membuka (decrypt) data tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (private key cryptography) atau dengan kunci yang berbeda (public key cryptography).



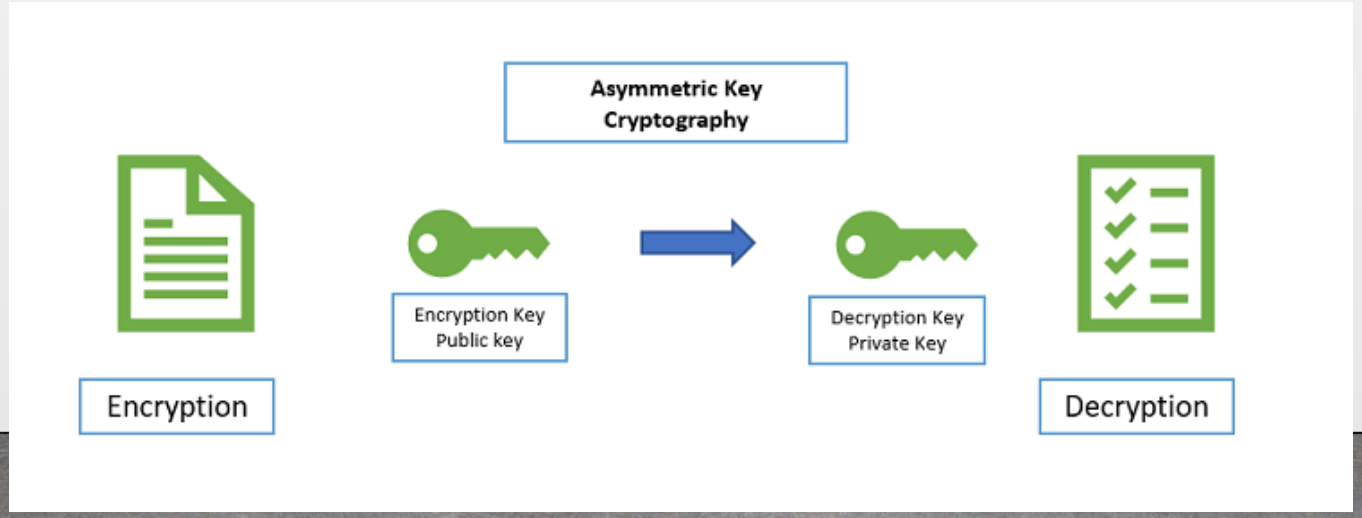
Kriptografi Simetris

- Disebut kriptografi simetris apabila melakukan enkripsi menggunakan kunci yang sama dengan saat nanti melakukan dekripsi.
- Kunci yang sama ini disebut dengan Secret Key atau Shared Secret.
- Saat ini chiper untuk kriptografi simetris yang paling handal adalah AES256 dimana saat ini telah digunakan pada keamanan Pemerintah AS



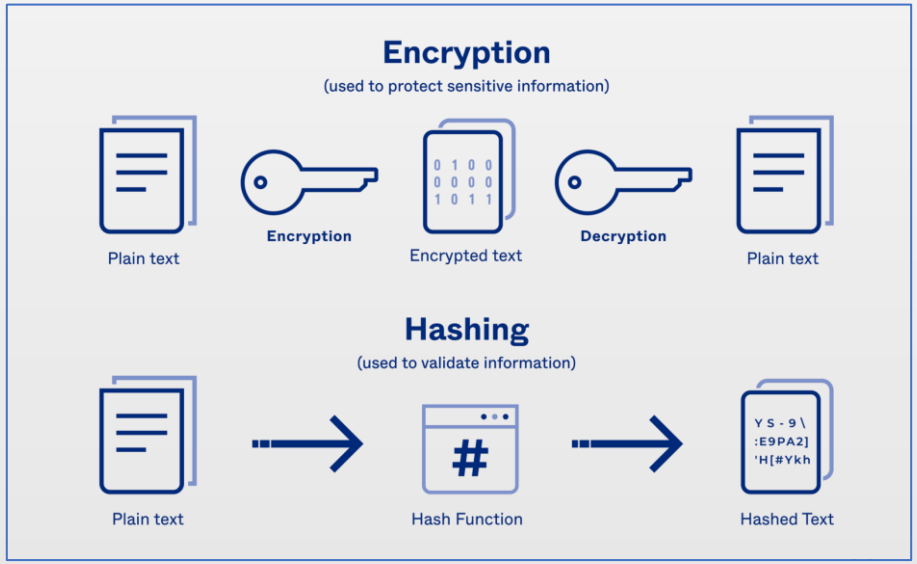
Kriptografi Asimetris

- Disebut kriptografi asimetris apabila dalam melakukan enkripsi dan dekripsi menggunakan dua kunci berbeda.
- Dua kunci ini disebut dengan public/private key. Jika sender ingin mengirim pesan yang dienkripsi maka menggunakan public key, sedangkan jika receiver ingin mendekripsi pesan dari sender maka digunakan private key.
- Sehingga public key ini harus diketahui sebelumnya oleh sender, agar sender bisa mengirim data secara rahasia ke receiver dan begitu pula sebaliknya
- Yang paling populer digunakan adalah algoritma RSA untuk melakukan kriptografi asimetris

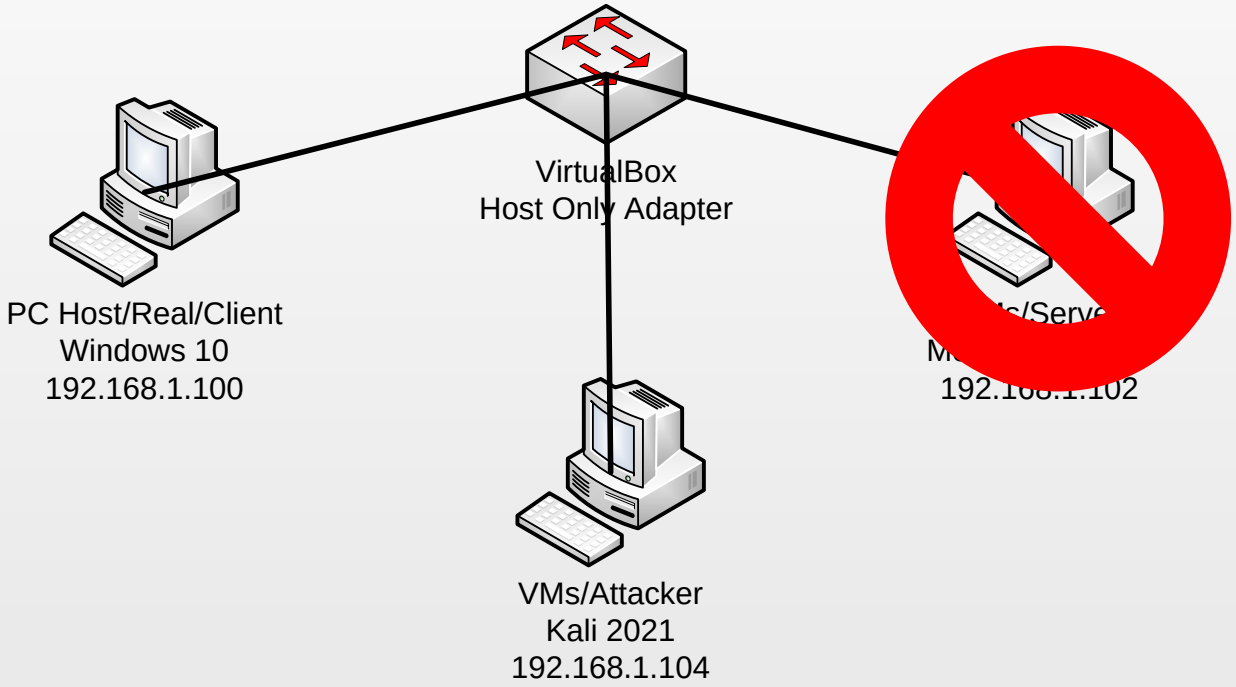


Konsep Hashing

- Hashing merupakan pemetaan suatu data menjadi deretan bit berukuran tetap secara acak.
- Hasil hashing bisa digunakan sebagai ringkasan data dan nilainya tidak bisa dikembalikan seperti semula.
- Sebenarnya ide awal hash digunakan untuk checksum suatu data. Untuk mengetahui integritas suatu data, tidak perlu mengecek keseluruhan data tapi cukup membandingkan nilai checksum dari hash.
- Namun perkembangannya hash bisa dijadikan fungsi kriptografi, misalkan untuk mengacak tampilan data password. Meskipun saat ini metode hash kurang aman namun tetap digunakan untuk melakukan checksum seperti MD5 atau SHA1



Topologi Skenario Jaringan Virtual



Setting SSH Server di Kali

```
┌──(nanza㉿nanzakali)-[~]
└─$ sudo systemctl status ssh                                                255 ×
[sudo] password for nanza:
○ ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
     Active: inactive (dead)
       Docs: man:sshd(8)
             man:sshd_config(5)
```

Aktifkan server SSH pada Kali. Hal ini digunakan agar Kali bisa transfer file dengan Windows. Lihat status SSH dengan systemctl status ssh, jika inactive berarti harus diaktifkan

```
┌──(nanza㉿nanzakali)-[~]
└─$ sudo systemctl enable ssh                                                  3 ×
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-instal
l.
Executing: /lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh
.service.
```

Enable layanan SSH dengan systemctl enable ssh

Setelah enable SSH, aktifkan SSH dengan systemctl start ssh

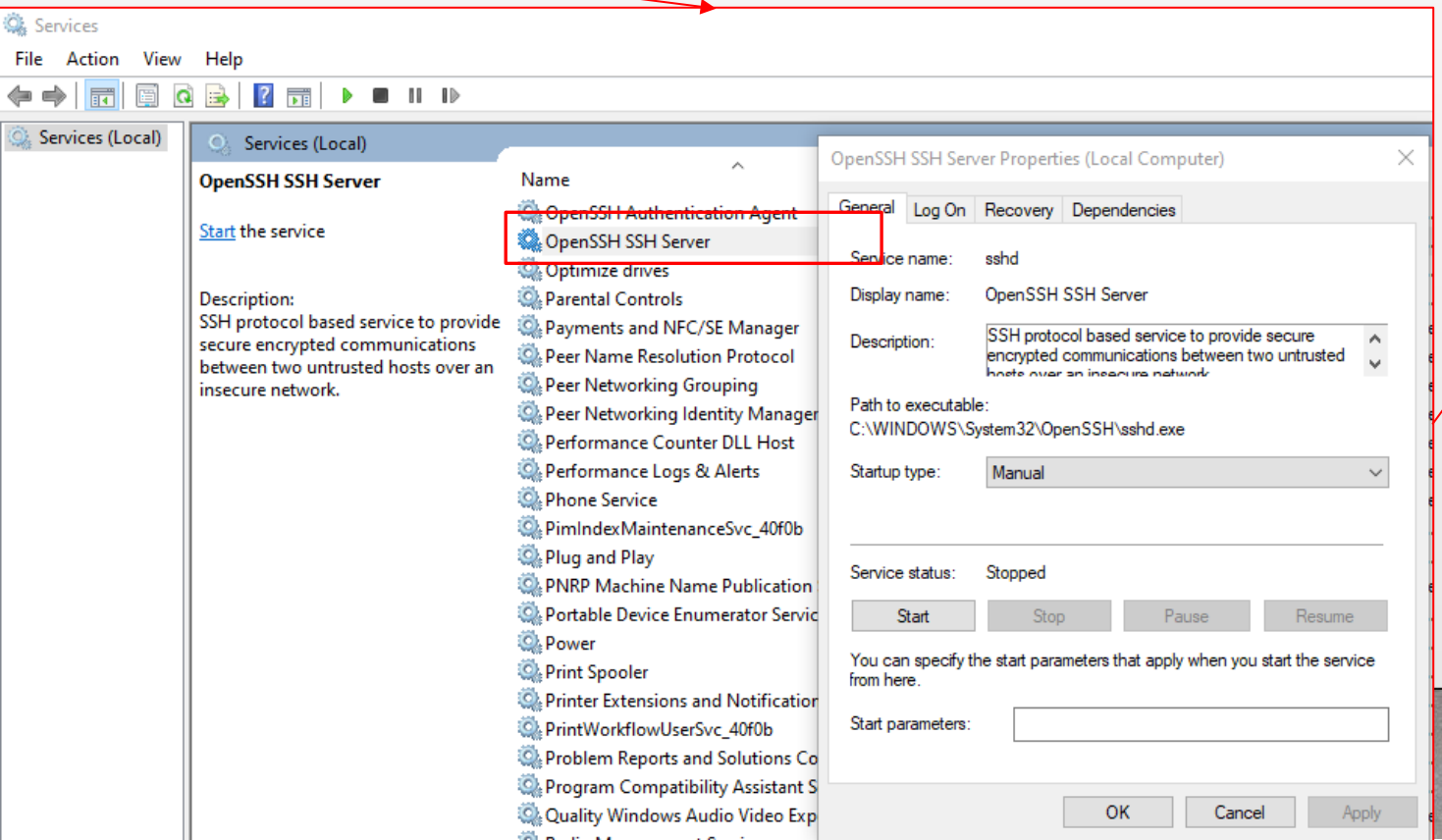
```
┌──(nanza㉿nanzakali)-[~]
└─$ sudo systemctl start ssh
```

```
┌──(nanza㉿nanzakali)-[~]
└─$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: disabled)
     Active: active (running) since Tue 2021-11-02 12:11:17 EDT; 14s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 1453 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1454 (sshd)
      Tasks: 1 (limit: 2294)
     Memory: 2.1M
        CPU: 38ms
     CGroup: /system.slice/ssh.service
             └─1454 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

Jika terdapat kata active maka server SSH telah aktif

Setting SSH Server di Windows 10

Begitupula dengan Windows, agar bisa saling transfer file melalui SSH maka perlu diaktifkan server SSH menggunakan OpenSSH Server dengan membuka Optional Features → pilih OpenSSH Server → **Restart Windows**




```
┌──(nanza㉿nanzakali)-[~]
└─$ nmap 192.168.1.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-02 12:47 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS i
em-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.100
Host is up (0.00044s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
```

Buka Kali dan lakukan scan port menggunakan NMAP. Pastikan SSH port 22 Windows telah Aktif

Setelah Windows aktif kembali buka Services → terdapat nama layanan OpenSSH SSH Server → klik 2x → pada jendela OpenSSH klik tombol Start agar layanan server SSH aktif

GNU PRIVACY GUARD (GPG)

Merupakan aplikasi yang menerapkan standar OpenPGP (Pretty Good Privacy) dimana seluruh Distro Linux telah dibekali dengan perintah GPG. Dengan GPG maka bisa menerapkan enkripsi baik secara simetris maupun asimetris

Enkripsi Simetris GPG Menggunakan AES256

```
┌──(nanza㉿nanzakali)-[~]
└─$ gpg --version
gpg (GnuPG) 2.2.27
libgcrypt 1.9.4
Copyright (C) 2021 Free Software Foundation, Inc.
License GNU GPL-3.0-or-later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /home/nanza/.gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2
```

Untuk melihat versi dan algoritma yang digunakan untuk kriptografi pada GPG, bisa menggunakan perintah gpg --version

```
┌──(nanza㉿nanzakali)-[~]
└─$ touch plaintext.txt

┌──(nanza㉿nanzakali)-[~]
└─$ ls
Desktop    Downloads  Pictures       Public          Templates
Documents  Music      plaintext.txt  scipag_vulscan  Videos
```

Buat file kosong dengan nama plaintext.txt melalui perintah touch

```
┌──(nanza㉿nanzakali)-[~]
└─$ nano plaintext.txt
```

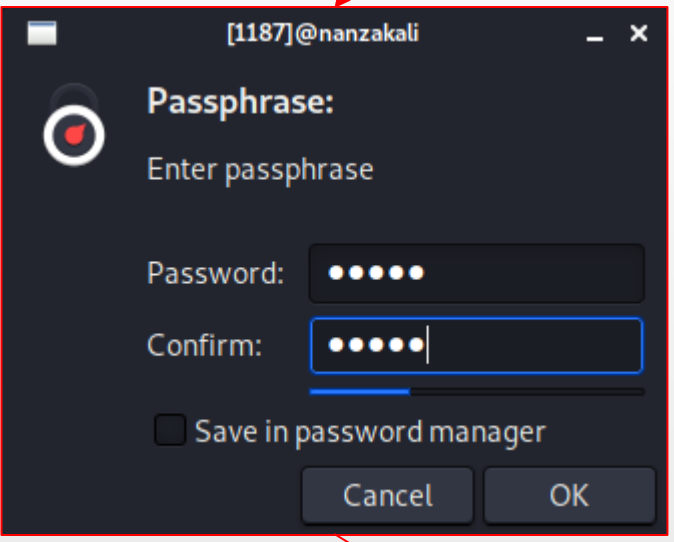
Isikan file plaintext.txt dengan editor nano

```
nanza@nanzakali: ~
File  Actions  Edit  View  Help
  GNU nano 5.8                          plaintext.txt *
text pada file ini adalah asli
akan digunakan enkripsi simetris
menggunakan algoritma AES256
```

Enkripsi Simetris GPG Menggunakan AES256

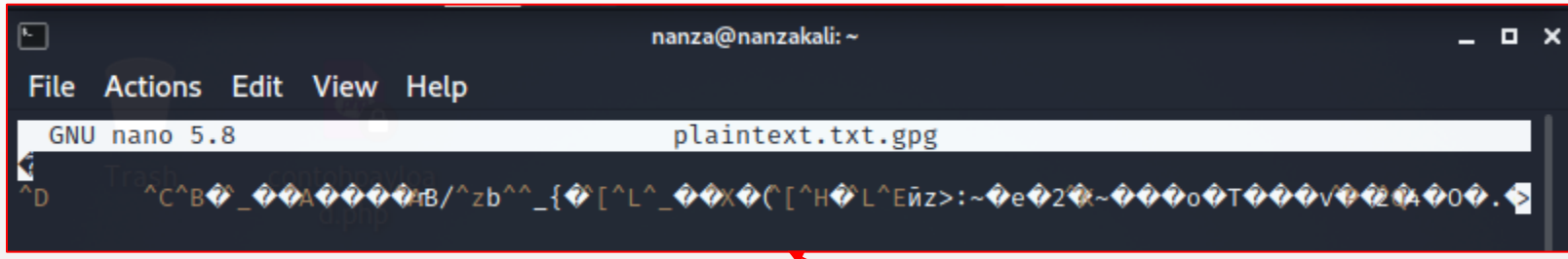
```
┌──(nanza㉿nanzakali)-[~]
└─$ gpg --symmetric --cipher-algo AES256 plaintext.txt
gpg: keybox '/home/nanza/.gnupg/pubring.kbx' created
```

Lakukan enkripsi simetris menggunakan metode AES256 pada plaintext.txt



Selanutnya akan disuruh memasukkan Passphrase. Passphrase ini adalah secret key untuk melakukan enkripsi maupun dekripsi

Namun isi telah berubah menjadi chipertext dimana sulit dipahami



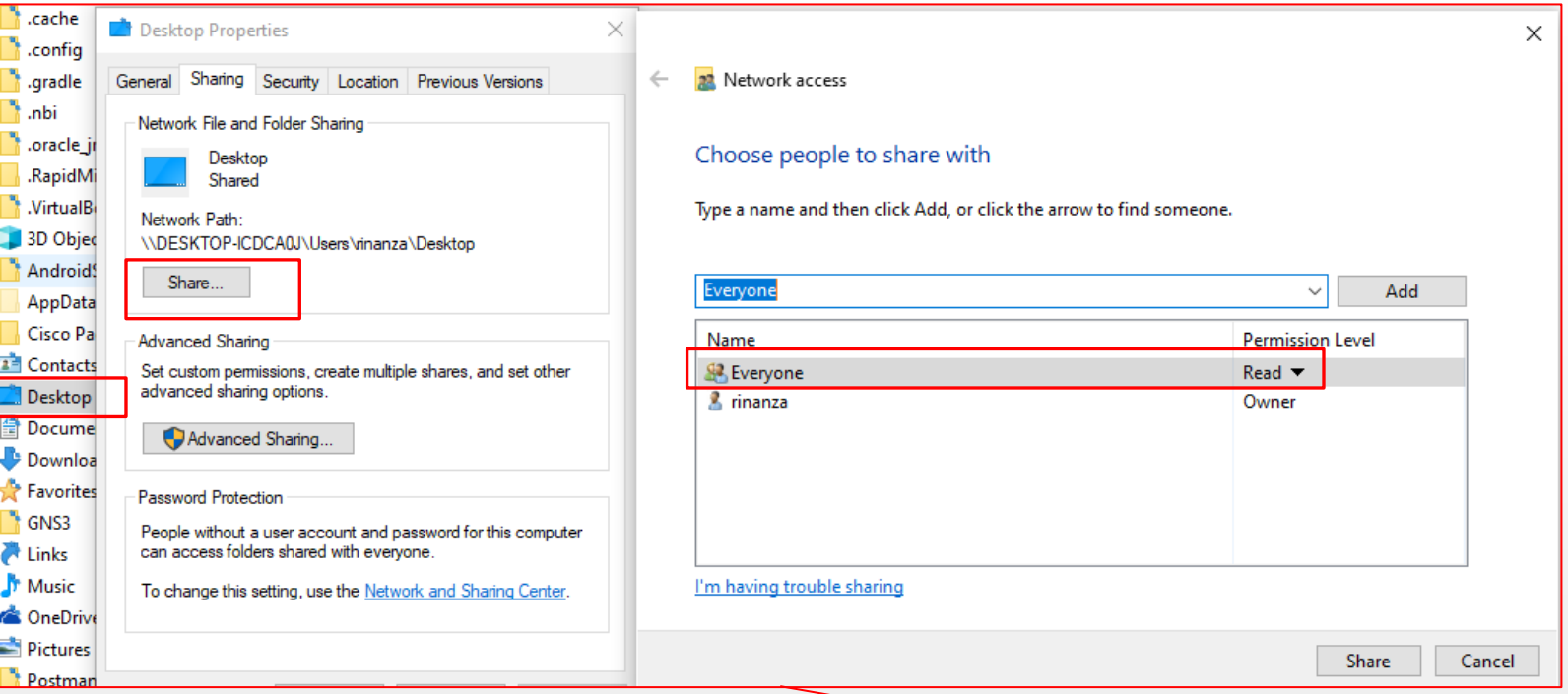

```
┌──(nanza㉿nanzakali)-[~]
└─$ nano plaintext.txt.gpg
```

Isi file .gpg bisa dilihat secara langsung menggunakan editor nano

Diperoleh output dengan format .gpg

```
┌──(nanza㉿nanzakali)-[~]
└─$ ls
Desktop    Downloads  Pictures        plaintext.txt.gpg  scipag_vulscan  Videos
Documents  Music      plaintext.txt   Public             Templates
```

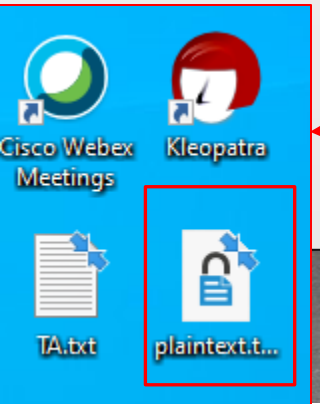
Enkripsi Simetris GPG Menggunakan AES256



Lakukan transfer data chipertext dari Kali menuju Windows melalui SSH. Misallkan target direktori adalah Desktop maka setting Desktop agar shareable dengan memberikan hak akses **read and write** pada user Everyone.

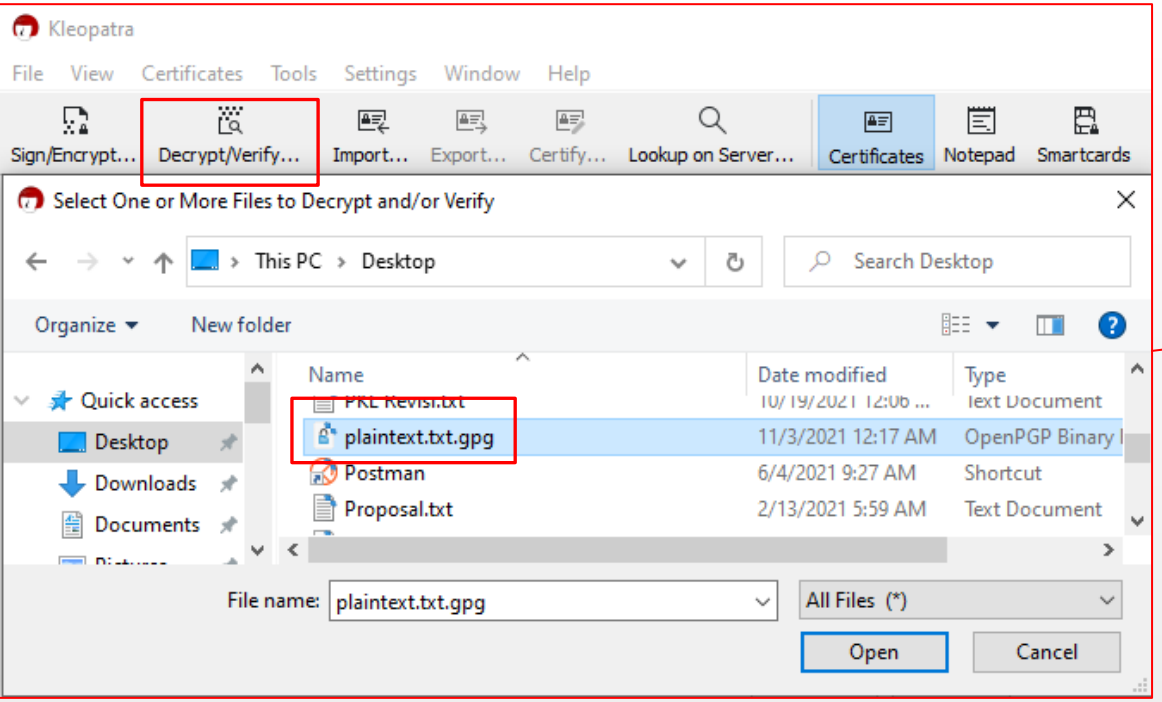
Pada Kali lakukan transfer file chipertext menggunakan perintah scp

```
┌──(nanza㉿nanzakali)-[~]
└─$ scp plaintext.txt.gpg rinanza@192.168.1.100:/C:/Users/rinanza/Desktop
rinanza@192.168.1.100's password:
plaintext.txt.gpg                             100%  162   106.2KB/s   00:00
```



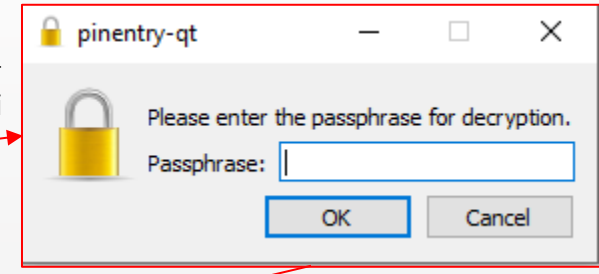
Pastikan file chipertext telah menuju Windows

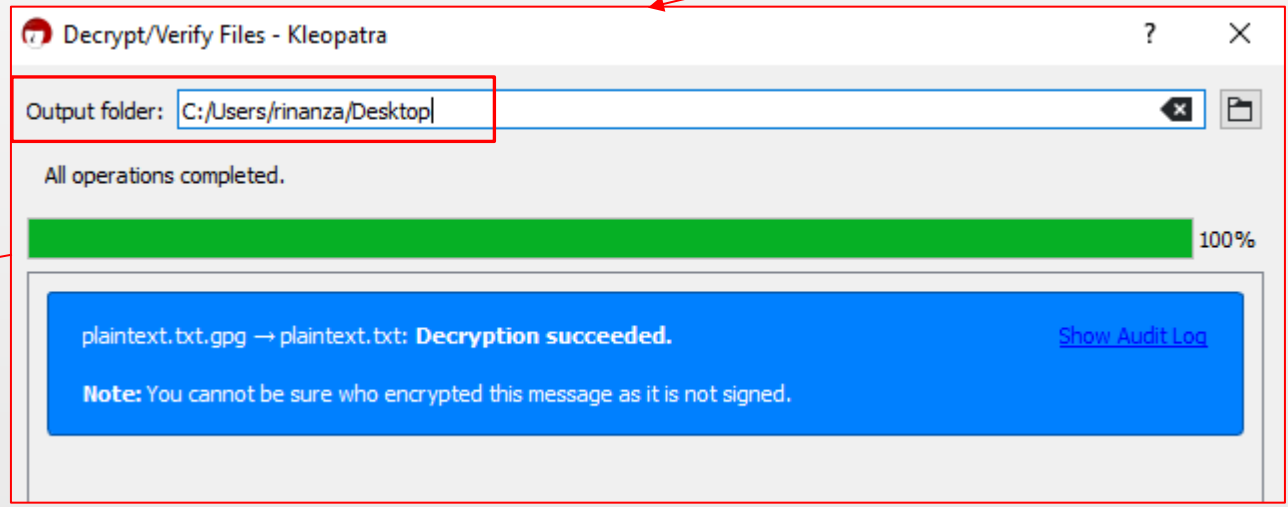
Enkripsi Simetris GPG Menggunakan AES256



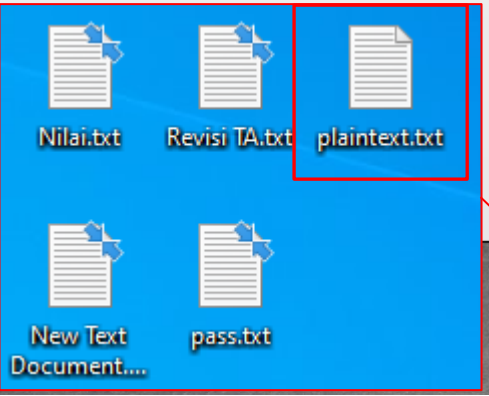
Buka GPGforWindows Manager Kleopatra → pilih menu Decrypt → buka chipertext yang akan didekripsi

Masukkan Passphrase yang sama nilainya seperti saat enkripsi





File plaintext akan tersimpan sesuai path pada Output Folder



Enkripsi Asimetris GPG Menggunakan RSA

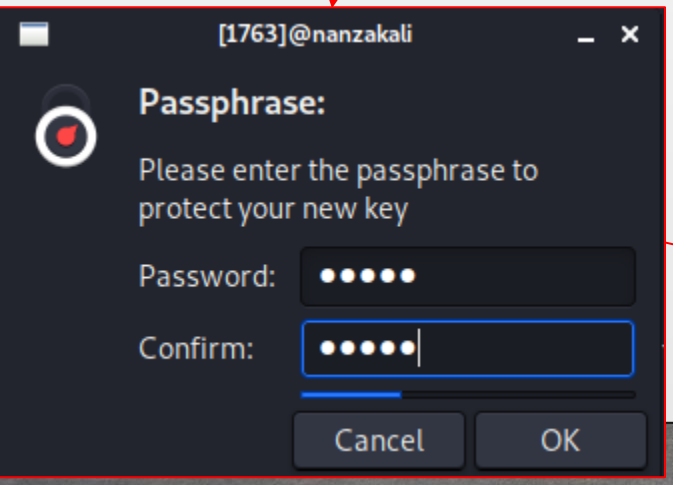
```
┌──(nanza㉿nanzakali)-[~]
└─$ gpg --gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Buat kunci menggunakan perintah –gen-key. Secara default menggunakan RSA

```
Real name: rinanza
Email address: rinanza@rinanza.com
You selected this USER-ID:
    "rinanza <rinanza@rinanza.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o
```

Masukkan nama dan alamat email. Data ini diunakan untuk memebuat karakter random dalam membuat kunci → jika sudah ok jawab dengan O



Sebelum selesai membuat kunci akan muncul pop-up untuk memasukkan Passphrase. Passphrase sebenarnya opsional

```
┌──(nanza㉿nanzakali)-[~]
└─$ gpg --list-secret-keys
/home/nanza/.gnupg/pubring.kbx
------------------------------
sec   rsa3072 2021-11-03 [SC] [expires: 2023-11-03]
      66E35F3BF02F6EB125BFDC079631AC1AB175C98E
uid           [ultimate] rinanza <rinanza@rinanza.com>
ssb   rsa3072 2021-11-03 [E] [expires: 2023-11-03]
```

Untuk melihat daftar private key gunakan perintah –list-secret-keys

```
┌──(nanza㉿nanzakali)-[~]
└─$ gpg --list-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 2023-11-03
/home/nanza/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2021-11-03 [SC] [expires: 2023-11-03]
      66E35F3BF02F6EB125BFDC079631AC1AB175C98E
uid           [ultimate] rinanza <rinanza@rinanza.com>
sub   rsa3072 2021-11-03 [E] [expires: 2023-11-03]
```

Untuk melihat public key gunakan perintah –list-keys

```
public and secret key created and signed.

pub   rsa3072 2021-11-03 [SC] [expires: 2023-11-03]
      66E35F3BF02F6EB125BFDC079631AC1AB175C98E
uid                      rinanza <rinanza@rinanza.com>
sub   rsa3072 2021-11-03 [E] [expires: 2023-11-03]
```

Key-pair akan terbuat baik private key maupun public key dengan nama rinanza

Enkripsi Asimetris GPG Menggunakan RSA

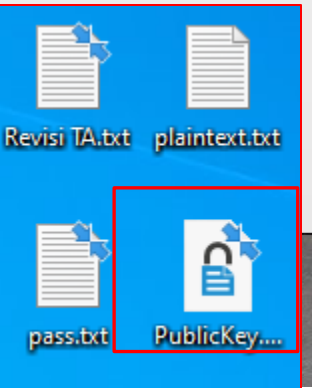
```
┌──(nanza㉿nanzakali)-[~]
└─$ gpg --export --armor rinanza > PublicKey.asc

┌──(nanza㉿nanzakali)-[~]
└─$ ls
Desktop    Downloads  Pictures       plaintext.txt.gpg  PublicKey.asc  Templates
Documents  Music      plaintext.txt  Public             scipag_vulscan  Videos
```

Ekspor public key atas nama rinanza menjadi file PublicKey.asc. Public key ini digunakan sender untuk melakukan enkripsi file

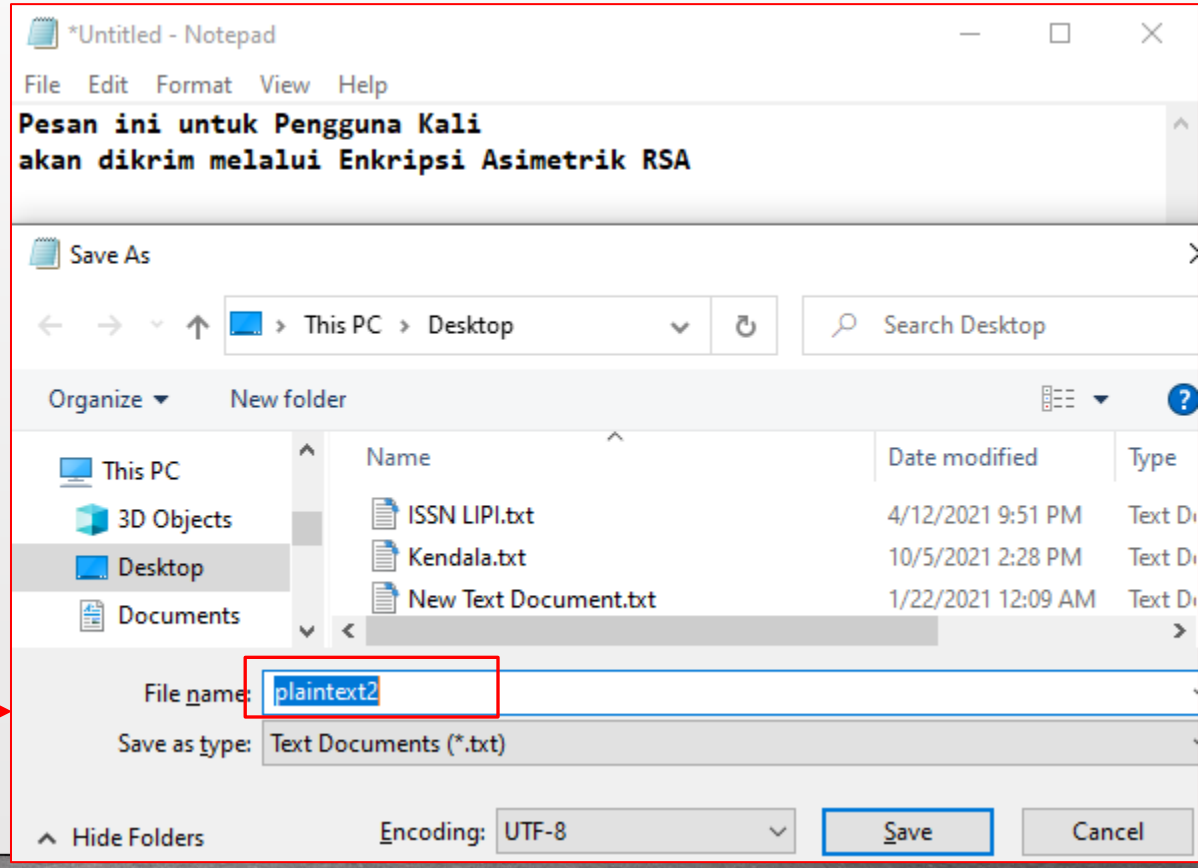
```
┌──(nanza㉿nanzakali)-[~]
└─$ scp PublicKey.asc rinanza@192.168.1.100:/C:/Users/rinanza/Desktop
rinanza@192.168.1.100's password:
PublicKey.asc                                 100% 2448     1.4MB/s   00:00
```

Sebagai sender dimisalkan adalah Windows, maka kirim public key dalam format .asc ke Windows menggunakan perintah scp

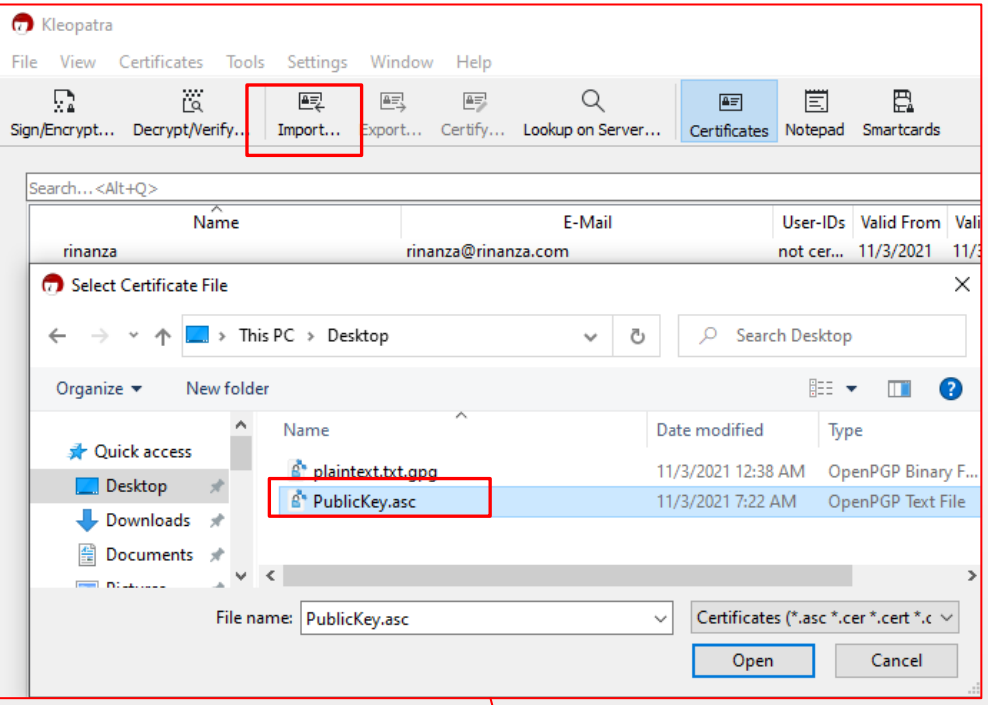


Pastikan public key telah berada pada Windows

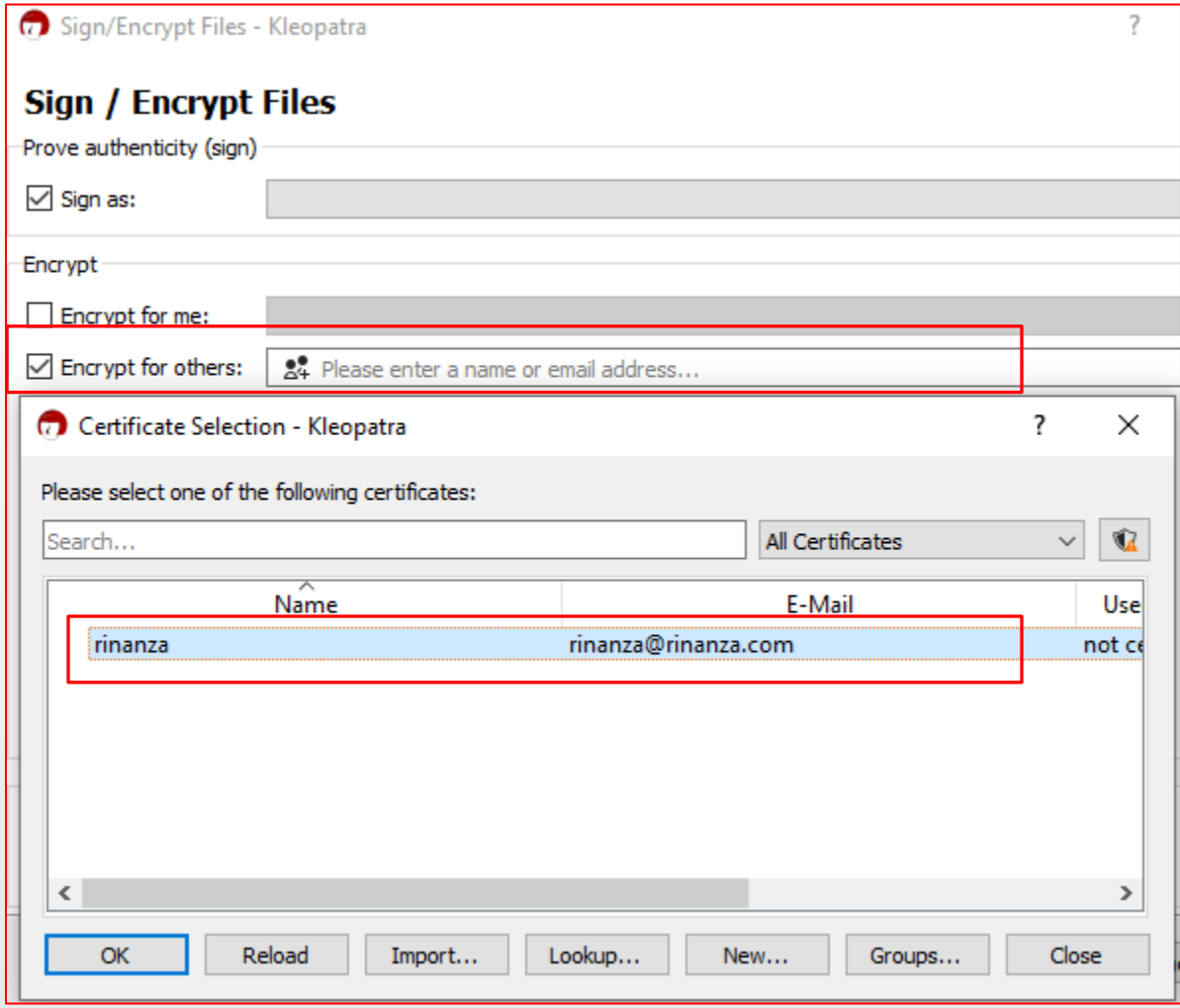
Dimisalkan sender Windows ingin mengirim file text yang disimpan dalam plaintext2.txt, maka dibuat file plaintext2.txt pada Windows



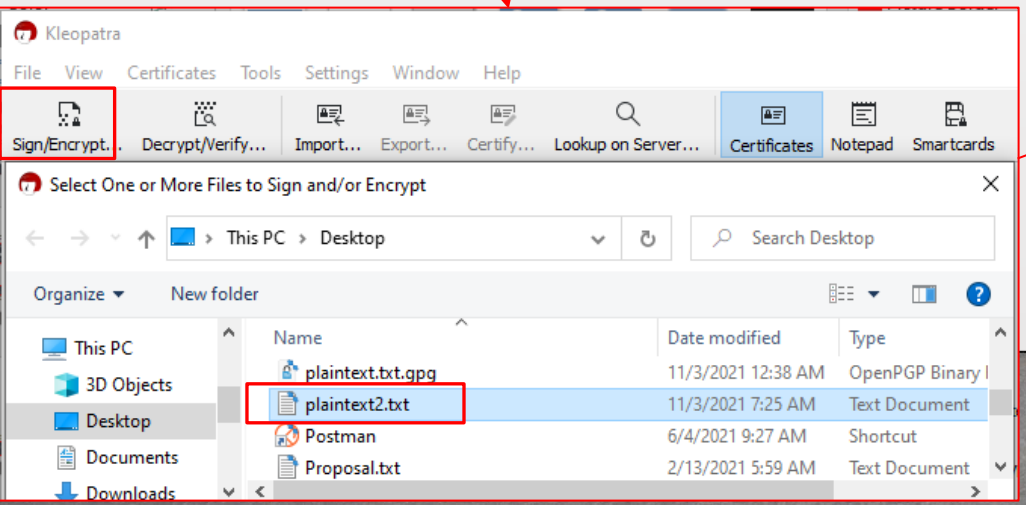
Enkripsi Asimetris GPG Menggunakan RSA



Buka GPGforWindows Manager Kleopatra → pilih menu Import Certificate → buka public key yang dikirim oleh Kali berupa PublicKey.asc → Open



Akan terbuka jendela Encrypt → pada form Encrypr For Others, pilih public key atas nama rinanza (sesuai dari Kali) → OK

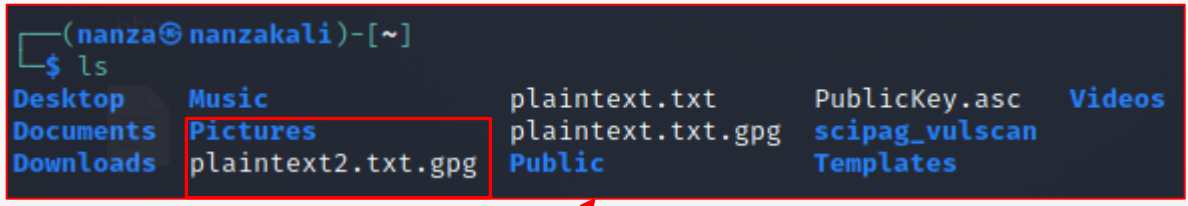


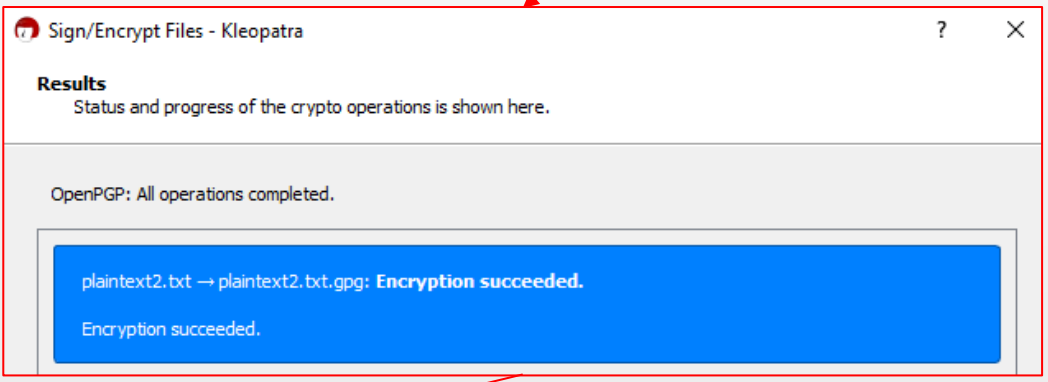
Pada Kleopatra → pilih menu Sign/Encrypt → pilih file text plaintext2.txt → Open

Enkripsi Asimetris GPG Menggunakan RSA

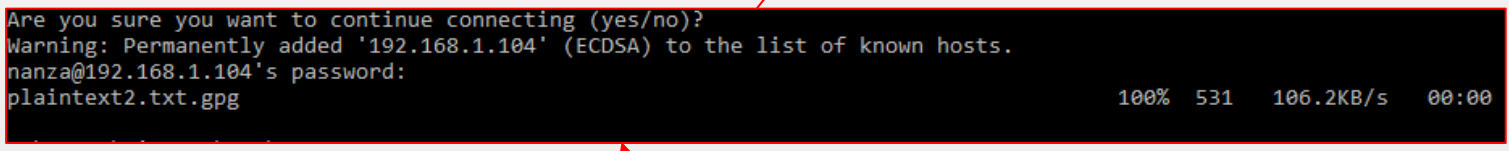
Pada Output pilih tempat chipertext dibuat dalam file bernama plaintext2.txt.gpg → Encrypt

Pastikan file chipertext benar ada di Kali

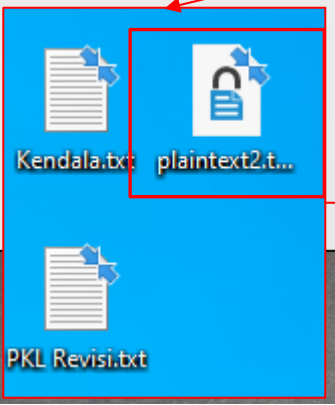




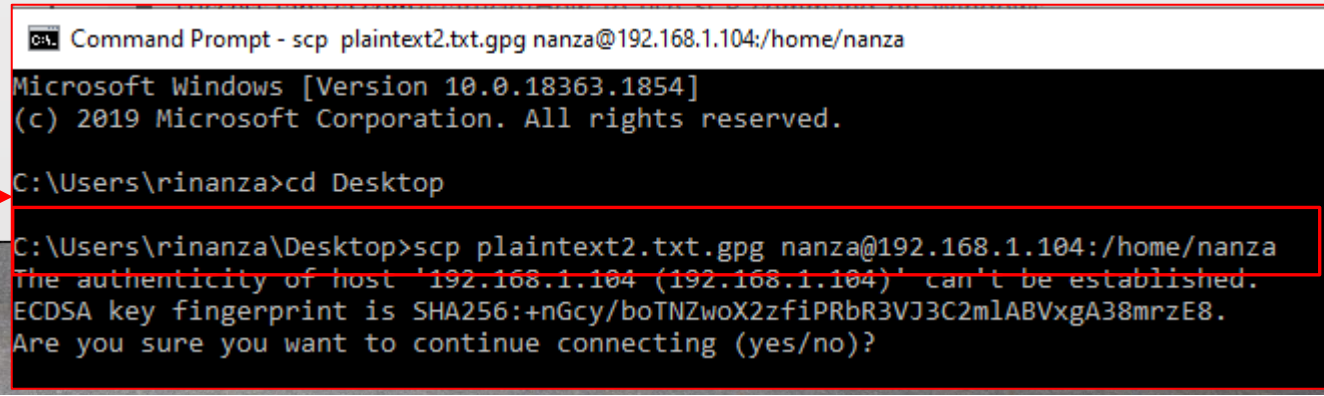
Pastikan telah berhasil dikirim



Kirim file chipertext plaintext2.txt.gpg menuju Kali menggunakan perintah scp pada CMD



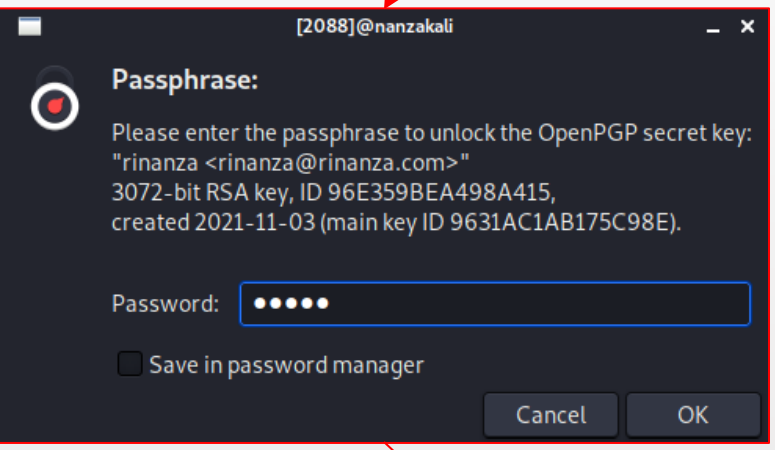
Pastikan file chipertext plaintext2.txt.gpg telah berhasil dibuat



Enkripsi Asimetris GPG Menggunakan RSA

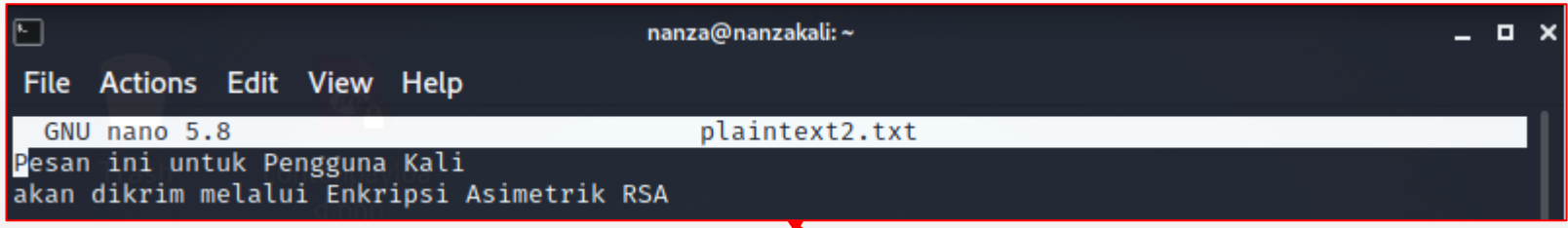
```
┌──(nanza㉿nanzakali)-[~]
└─$ gpg --output plaintext2.txt --decrypt plaintext2.txt.gpg
```

Dekripsi file chipertext dengan perintah –decrypt dengan output plaintext2.txt



Karena saat membuat pair key menambahkan Passphrase maka untuk melakukan dekripsi harus memasukkan Passphrase yang sama

Isinya sesuai dengan sender dari Windows




```
┌──(nanza㉿nanzakali)-[~]
└─$ nano plaintext2.txt
```

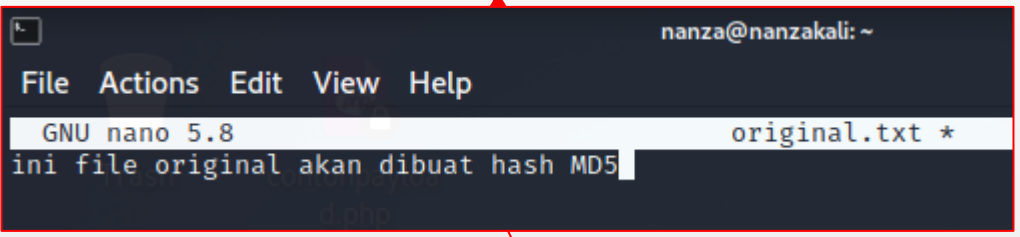
```
┌──(nanza㉿nanzakali)-[~]
└─$ ls
Desktop    Music            plaintext2.txt.gpg  Public          Templates
Documents  Pictures         plaintext.txt       PublicKey.asc   Videos
Downloads  plaintext2.txt   plaintext.txt.gpg   scipag_vulscan
```

Dekripsi berupa plaintext plaintext2.txt telah berhasil

Cek Integritas File dengan Hash MD5

```
┌──(nanza㉿nanzakali)-[~]
└─$ touch original.txt
```

Buat sebuah file txt dengan nama original.txt



Isikan konten teks pada original.txt → simpan

```
┌──(nanza㉿nanzakali)-[~]
└─$ md5sum original.txt > hashfile.txt

┌──(nanza㉿nanzakali)-[~]
└─$ ls
Desktop    Downloads     Music       Pictures  scipag_vulscan  Videos
Documents  hashfile.txt  original.txt  Public    Templates

┌──(nanza㉿nanzakali)-[~]
└─$ cat hashfile.txt
d42266680290c6084691832686cadce8  original.txt
```

Lakukan hashing dengan perintah md5sum pada original.txt → kemudaian nila hash masukkan ke hashfile txt dengan redirect >

Lakukan hashing kembali dengan perintah md5sum pada duplicate.txt → masukkan nilai sum menuju hashfile.txt menggunakan append >> → saat dibuka hashfile.txt terlihat jelas bahwa hash original txt dan duplicate.txt sama

```
┌──(nanza㉿nanzakali)-[~]
└─$ md5sum duplicate.txt >> hashfile.txt

┌──(nanza㉿nanzakali)-[~]
└─$ cat hashfile.txt
d42266680290c6084691832686cadce8  original.txt
d42266680290c6084691832686cadce8  duplicate.txt
```

Salin file original.txt ke file dengan nama duplicate.txt

```
┌──(nanza㉿nanzakali)-[~]
└─$ cp original.txt duplicate.txt

┌──(nanza㉿nanzakali)-[~]
└─$ ls
Desktop    Downloads     hashfile.txt  original.txt  Public          Templates
Documents  duplicate.txt  Music         Pictures      scipag_vulscan  Videos
```

Cek Integritas File dengan Hash MD5

```
┌──(nanza㉿nanzakali)-[~]
└─$ pwd >> duplicate.txt

┌──(nanza㉿nanzakali)-[~]
└─$ cat duplicate.txt
ini file original akan dibuat hash MD5
/home/nanza
```

Lakukan perubahan file text duplicate.txt dengan menambah hasil perintah PWD dengan append >>

```
┌──(nanza㉿nanzakali)-[~]
└─$ md5sum duplicate.txt >> hashfile.txt

┌──(nanza㉿nanzakali)-[~]
└─$ cat hashfile.txt
d42266680290c6084691832686cadce8  original.txt
d42266680290c6084691832686cadce8  duplicate.txt
0df7152ddc5c7196ab6c12a48041d446  duplicate.txt
```

Lakukan hashing dengan perintah md5sum pada file duplicate.txt → kemudian simpan hasilnya ke hashfile.txt dengan append >> → jika dilihat isi hashfile.txt terlihat bahwa nilai hash pada duplicate.txt terakhir berubah

Untuk melihat integritas hash bisa menggunakan perintah --check

```
┌──(nanza㉿nanzakali)-[~]
└─$ md5sum --check hashfile.txt original.txt
original.txt: OK
duplicate.txt: FAILED
duplicate.txt: OK
md5sum: WARNING: 1 computed checksum did NOT match
md5sum: original.txt: no properly formatted MD5 checksum lines found
```

TUGAS

Buat video rekaman praktik dengan tugas:

- Lakukan Kriptografi Asimetrik untuk pertukaran data text berisi Nama, NIM, dan Alamat menggunakan metode RSA
- Lakukan praktik skenario checksum pda text berisi Nama, NIM, dan Alamat menggunakan SHA1

TERIMAKASIH