Nama : Dwi Luki Arisandy

Nim : 1310651061

Kelas : A

1. Cryptography

- Pengertian Kriptografi.

Kriptografi adalah sebuah pesan rahasia untuk menjalankan sebuah komunikasi yang aman. Tujuan dari Kriprografi yaitu mengamankan sebuah pesan yang dikirim oleh seorang pengirim dan pesan tersebut hanya bisa dimengerti dan dipahami oleh penerima yang dituju.

- Konsep Kriptology

Kriptology Merupakan sebuah komunikasi yang aman. Kriptology juga menciptakan sebuah pesan dengan isi pesan yang tersembunyi, supaya pesan tersebut hanya dapat dibuka oleh penerima tujuan.

Dalam Konsep Kriptology cipher adalah sebuah algoritma kriptografi dimana plaintext adalah pesan yang terenkripsi yang kemudian pesan tersebut dienkripsi sehingga mengubah dari plaintext ke chipertext. Lalu Deskripsi mengembalikan pesan chipertext kedalam plaintext (pesan awal).

- Jenis Kriptografi

Dalam kriptografi ada 3 jenis tentang Kriptografi yaitu Simetris, Asimetris dan Hash. Berikut penjelasan tentang masing-masing jenisnya :

1) Simetris

Algoritma simetris atau disebut juga algoritma Kriptografi konvensional adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses dekripsi. Algoritma Kriptografi simetris dibagi menjadi 2 kategori yaitu algoritma aliran (Stream Ciphers) dan algoritma blok (Block Ciphers). Pada algoritma aliran, proses penyandiannya berorientasi pada satu bit atau satu byte data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau byte data (per blok). Contoh algoritma kunci simetris adalah DES (Data Encryption Standard), blowfish, twofish, MARS, IDEA, 3DES (DES diaplikasikan 3 kali), AES (Advanced Encryption Standard) yang bernama asli Rijndael.

2) Asimetrik

Kriptografi asimetrik (asymmetric cryptography) adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Kunci enkripsi dapat disebarkan kepada umum dan dinamakan sebagai kunci publik (public key) sedangkan kunci dekripsi disimpan untuk digunakan sendiri dan dinamakan sebagai kunci pribadi (private key). Oleh karena itulah, Kriptografi ini dikenal pula dengan nama Kriptografi kunci publik (public key

cryptography). Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA (Riverst Shamir Adleman) dan ECC (Elliptic Curve Cryptography).

3) Hashing

Sering juga disebut fungsi enkripsi satu arah, atau disebut juga message diggest. Fungsi hash digunakan untuk menjamin servis otentikasi dan integritas suatu pesan atau file. Suatu fungsi hash h memetakan bit-bit string dengan panjang sembarang ke sebuah string dengan panjang tertentu misal n. Dengan domain D dan range R maka: Proses hashing merupakan proses pemetaan suatu input string menjadi output disebut. Output dari fungsi hash disebut nilai hash atau hasil hash.

- Serangan Kriptografi

Serangan kriptografi biasanya digunakan oleh kriptanalist untuk menemukan plaintext tanpa sebuah key atau kunci terhadap plaintext tersebut. Berikut berbagai macam serangan terhadap kriptografi :

1) Brute force
2) Known plaintext
3) Chosen plaintext and adaptive-chosen plaintext
4) Chosen ciphertext and adaptive-chosen ciphertext
5) Rubber-hose cryptanalysis

- Implementasi Kriptografi

Jenis-jenis kriptografi dapat diimplementasikan kedalam berbagai macam, contohnya

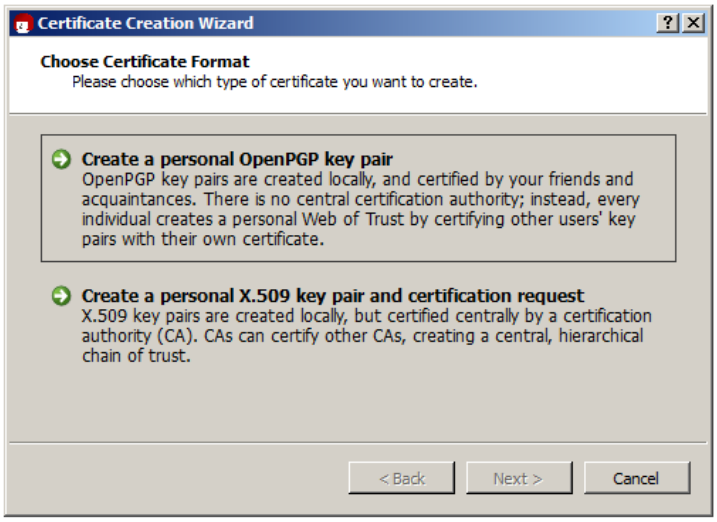
1) Digital Signature

Tanda tangan digital digunakan untuk dokumentanda kriptografi. tanda tangan digital memberikan nonrepudiation, yang mencakupotentikasi identitas penandatangan, dan bukti integritas dokumen (membuktikandokumen tidak berubah). Ini berarti pengirim tidak dapat menyangkal nanti(atau menolak) menandatangani dokumen.

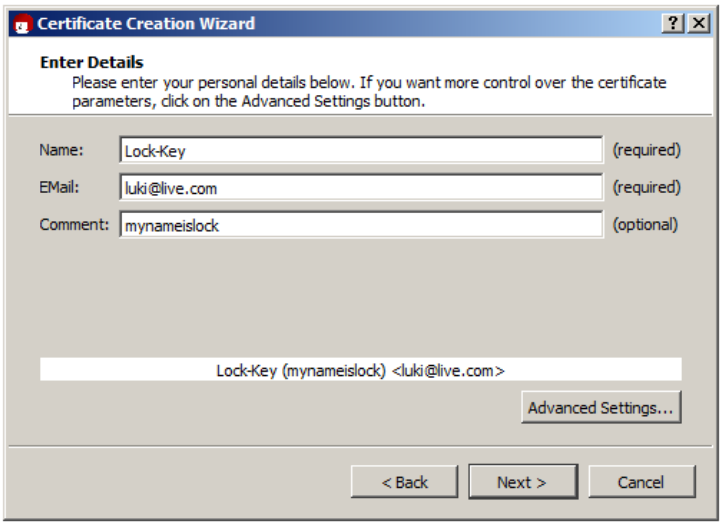
2) Public Key Infrastructure
3) Certificate Authorities and Organizational Registration Authorities
4) Certificate Revocation Lists
5) Key management issues
6) SSL and TLS

2. Software Encrypt Decrypt Menggunakan Gpg4win.

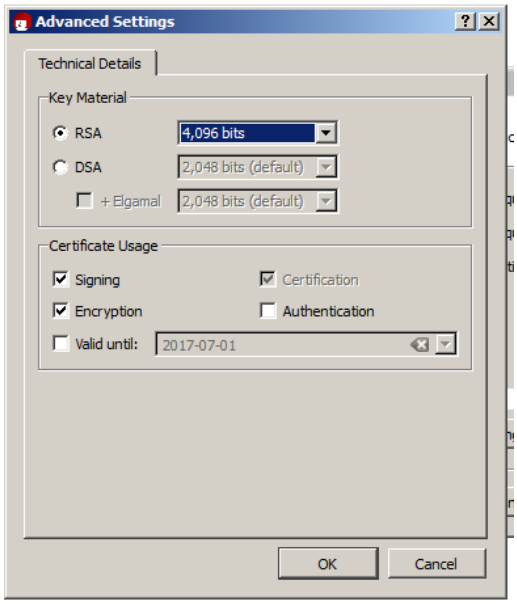
1. Pembuatan Sertifikat melalui software Kleopatra, klik pada Create a personal



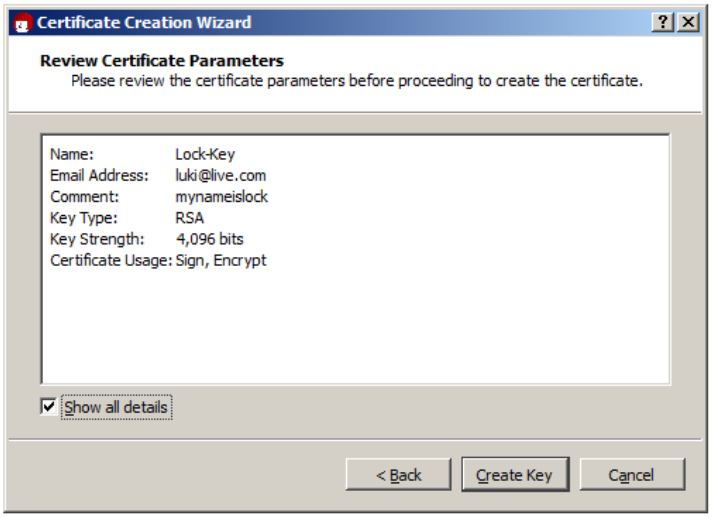
2. Selanjutnya isi Nama, Email dan komentar pada tujuan yang dikirim.



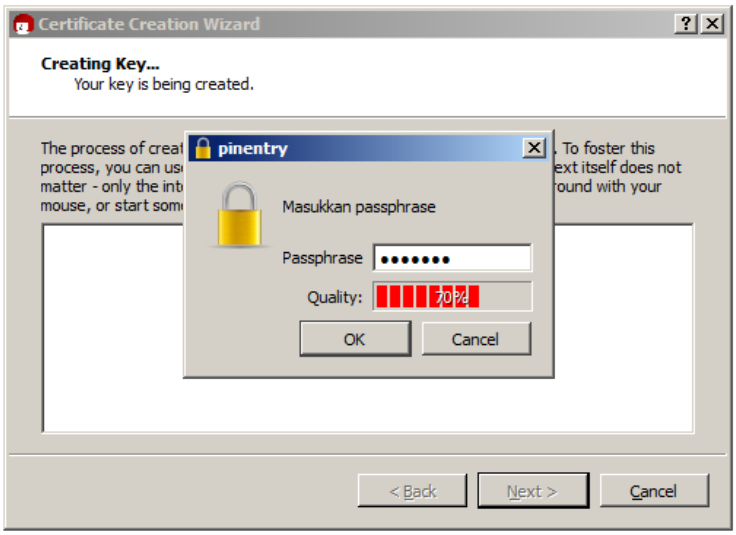
3. Ganti pada bagian RSA menjadi seperti digambar.



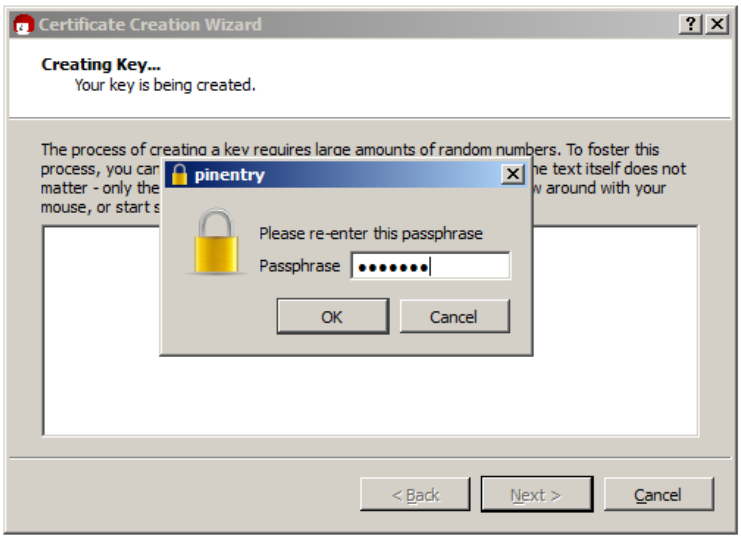
4. Selanjutnya Klik Create Key



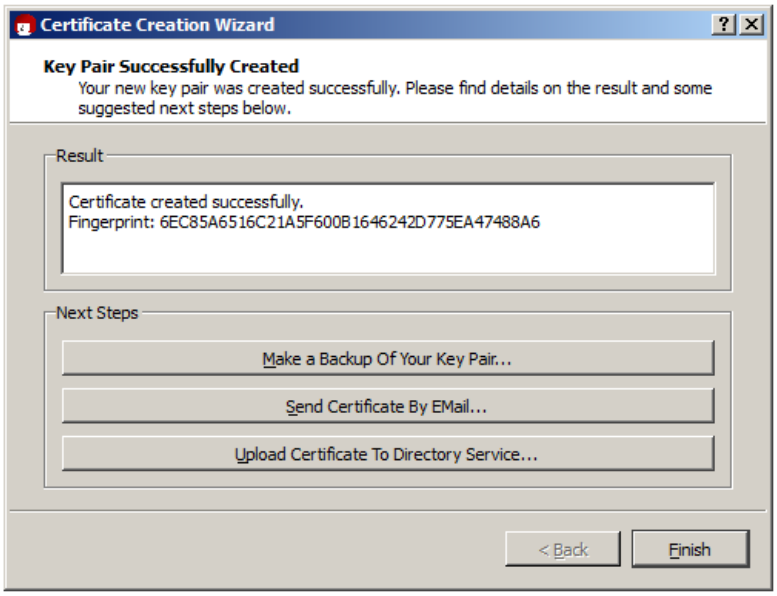
5. Masukkan password untuk sertifikatnya. Lalu klik ok.



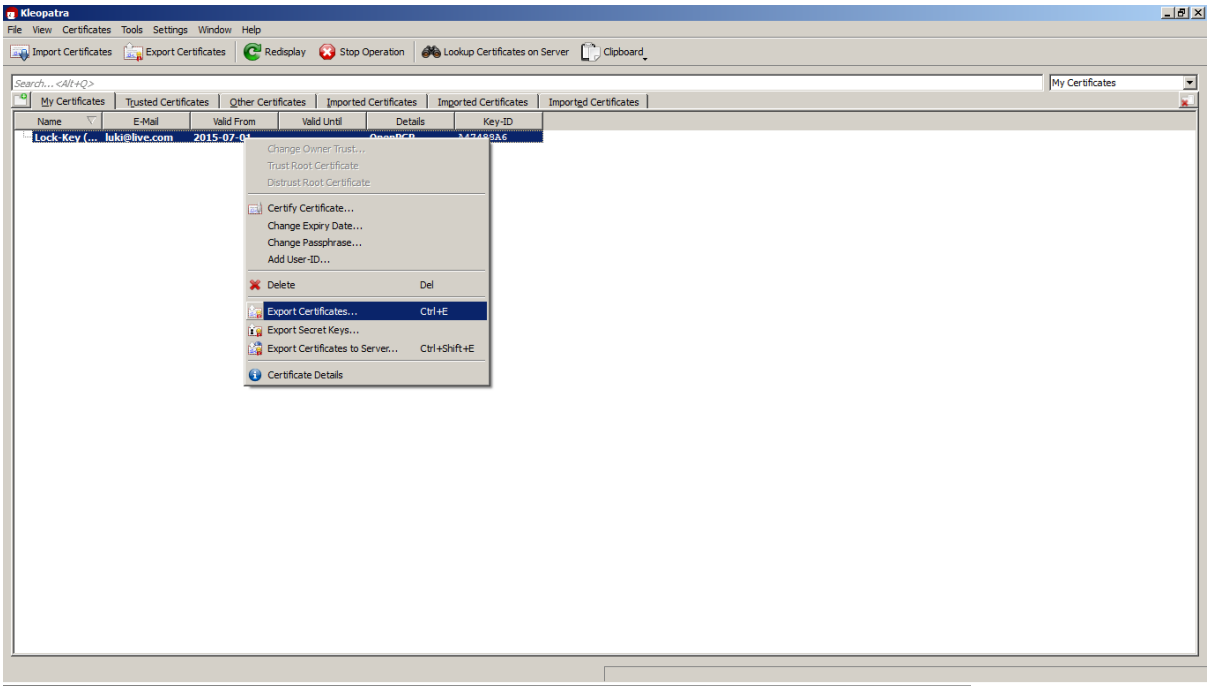
6. Masukkan ulang password untuk sertifikat. Klik ok

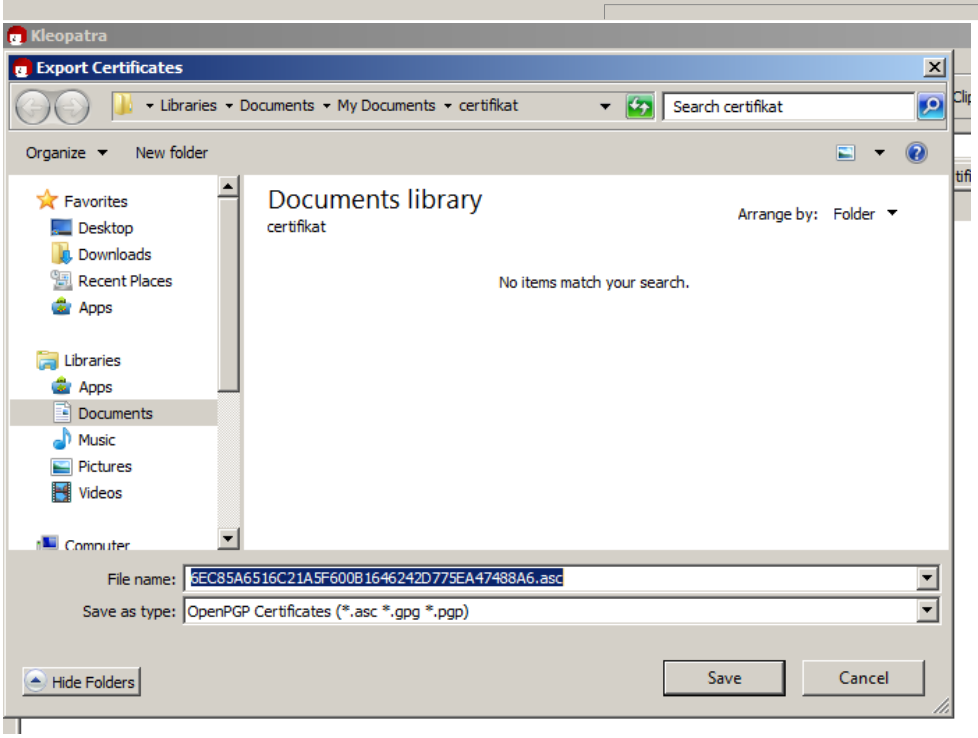


7. Klik finis, untuk selesai membuat sertifikat.

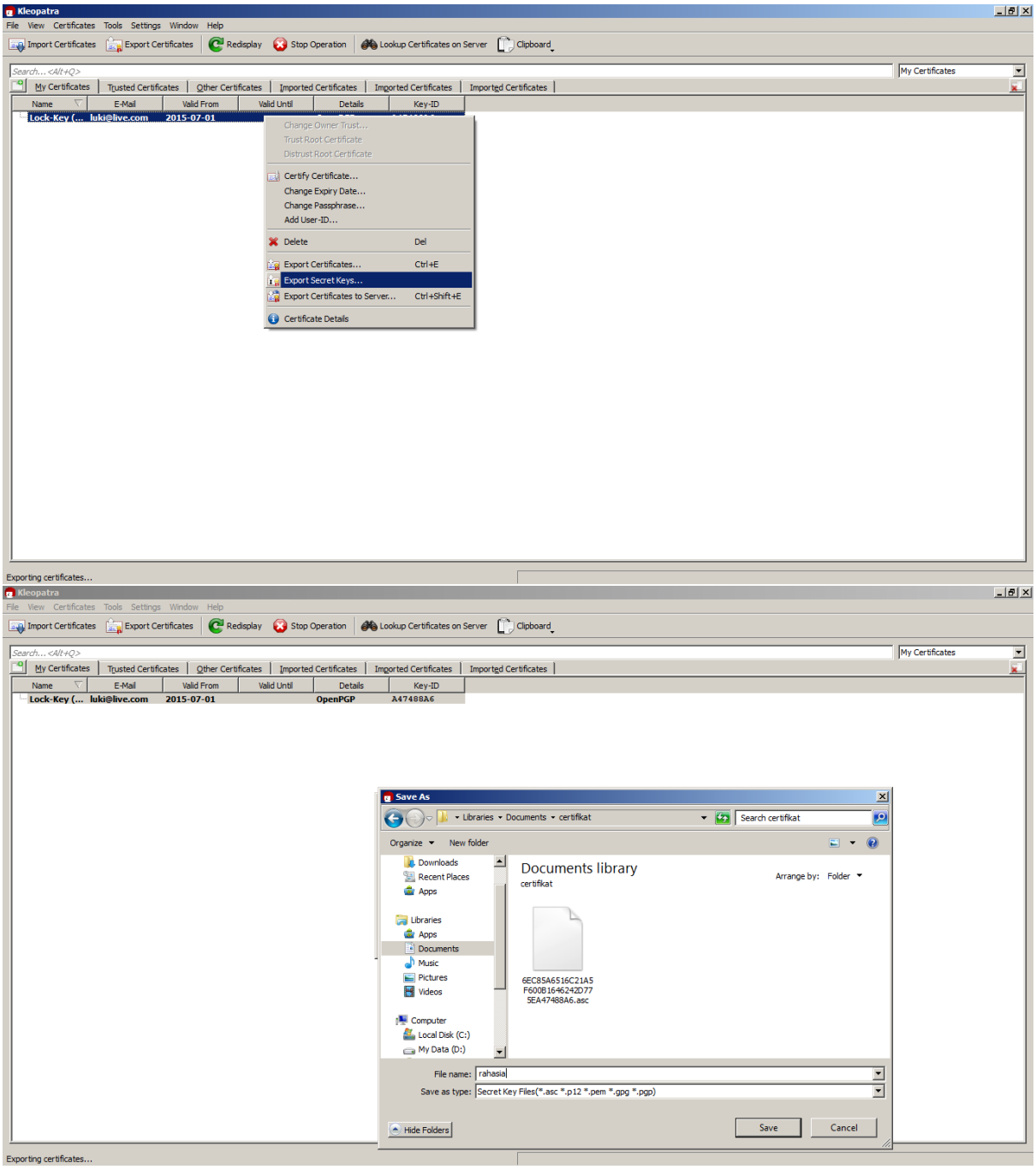


8. Selanjutnya export sertifikat dan simpan kedalam folder yang diinginkan. Klik save.

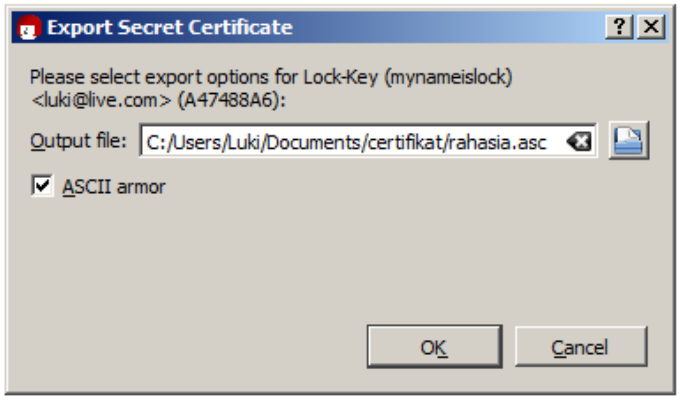


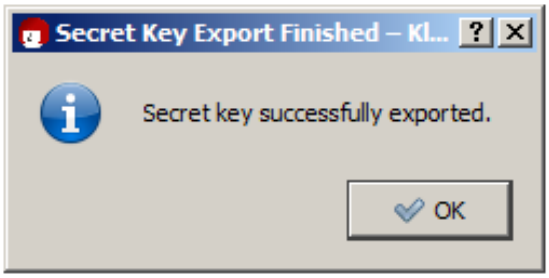


9. Selanjutnya export Secret key atau kunci rahasia kedalam salah satu folder yang telah disimpan sertifikat. Beri nama lalu klik save.

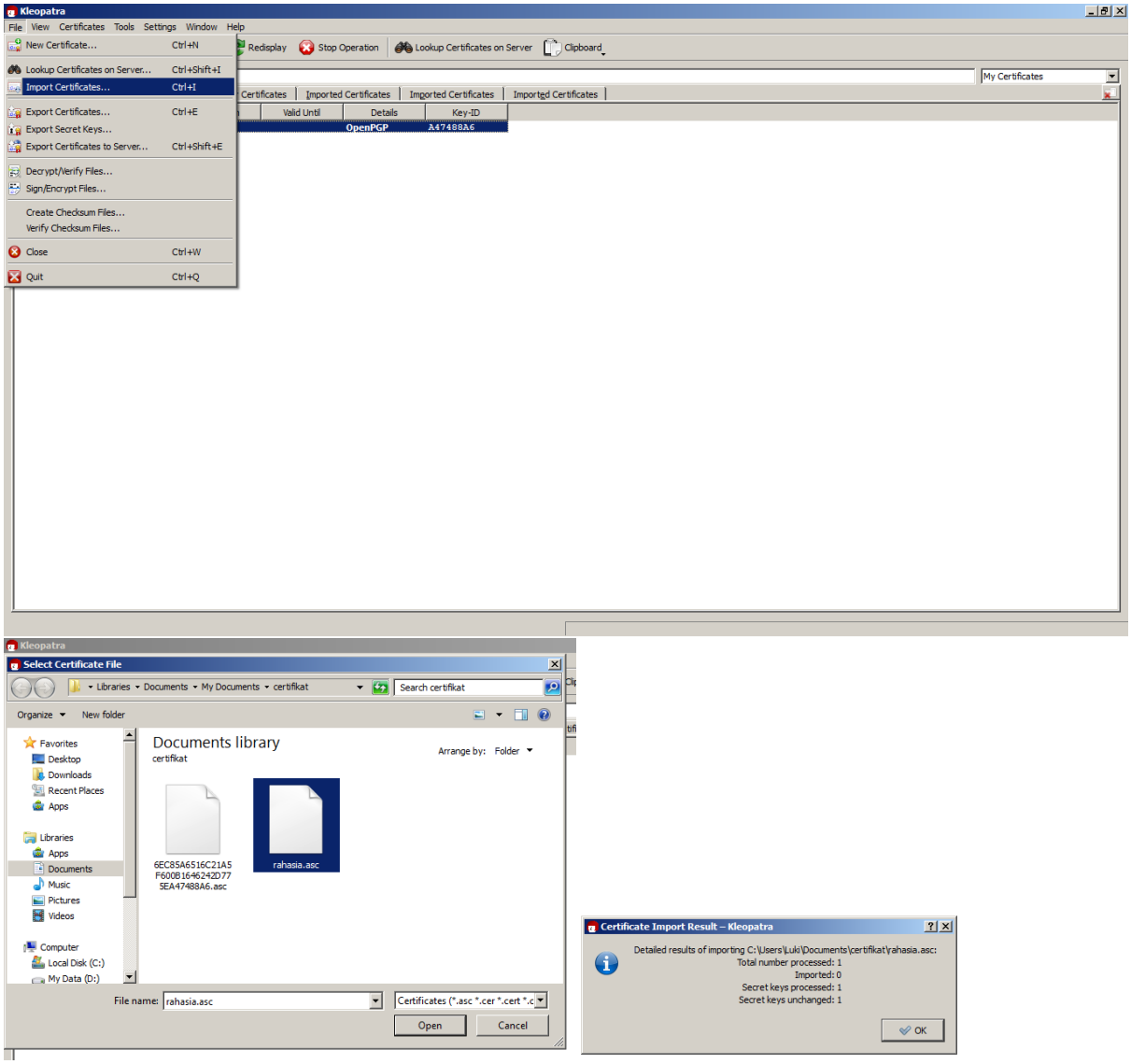


10. Centan pada ASCII lallu klik ok.

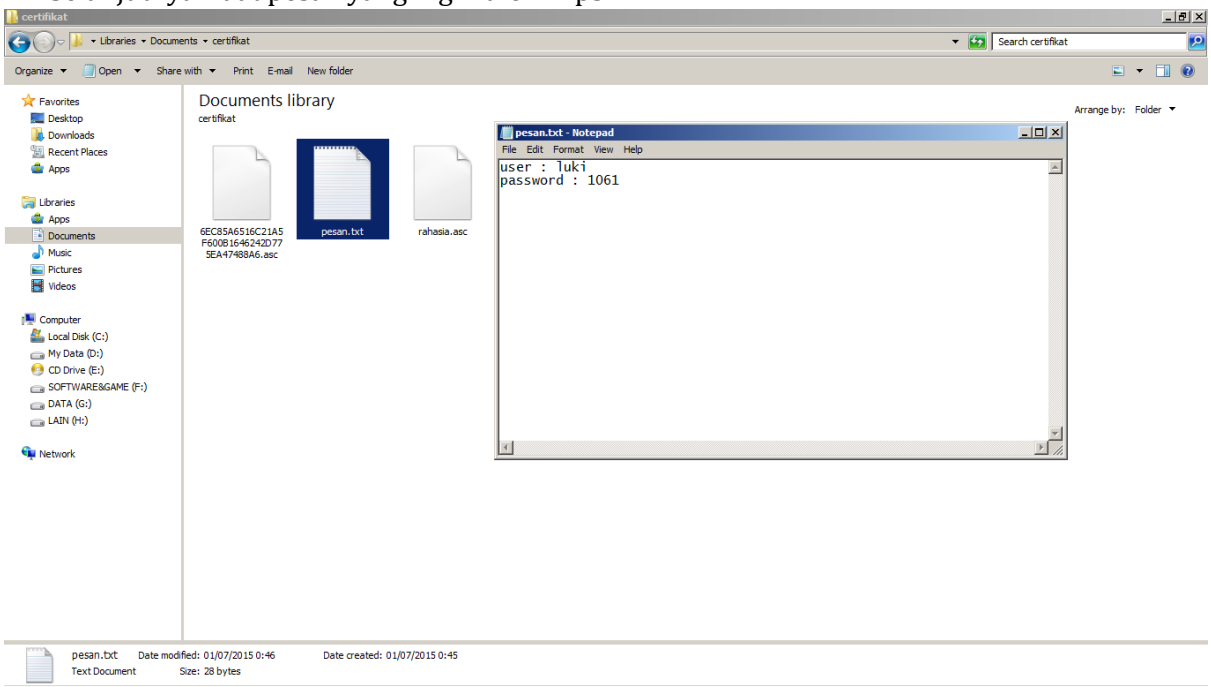




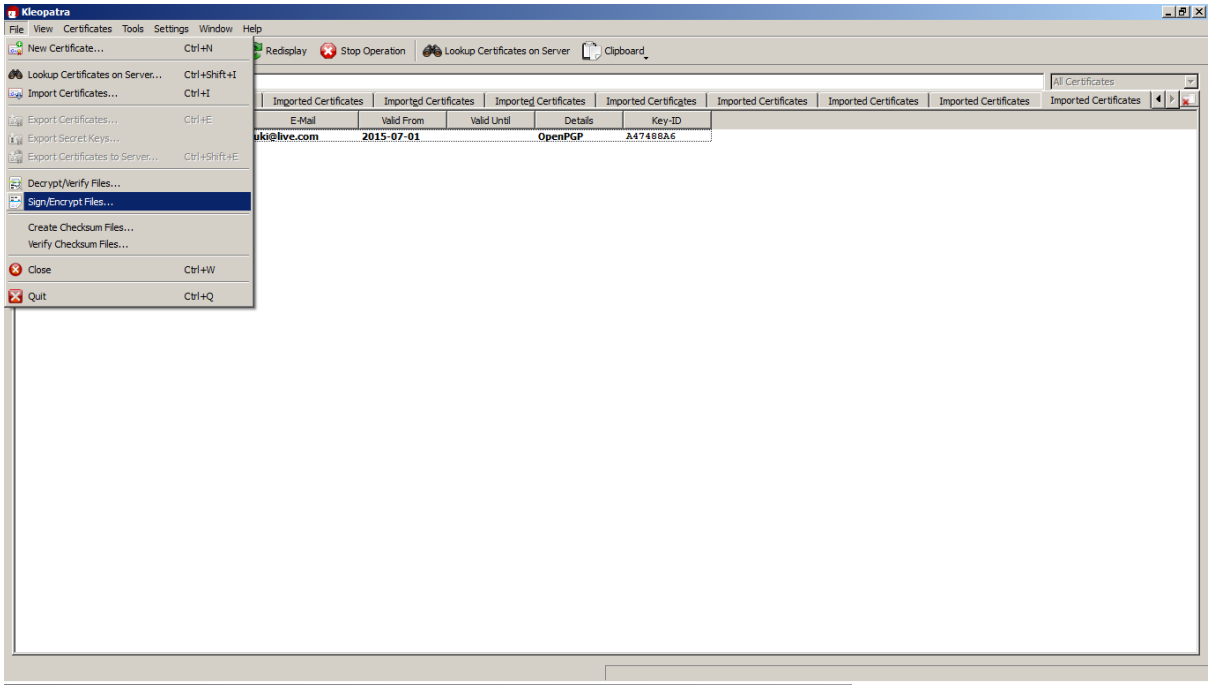
11. selanjutnya import sertifikat yang telah dibuat. Klik file > import Certificates > pilih rahasia.asc > lalu klik open.

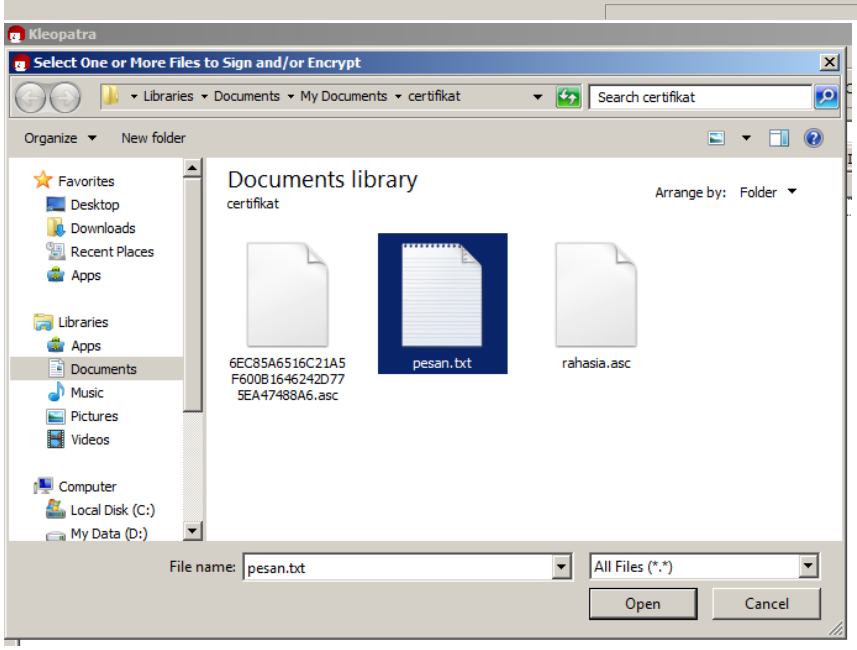

Kleopatra
File View Certificates Tools Settings Window Help
New Certificate... Ctrl+N
Lookup Certificates on Server... Ctrl+Shift+I
Import Certificates... Ctrl+I
Export Certificates... Ctrl+E
Export Secret Keys...
Export Certificates to Server... Ctrl+Shift+E
Decrypt/Verify Files...
Sign/Encrypt Files...
Create Checksum Files...
Verify Checksum Files...
Close Ctrl+W
Quit Ctrl+Q
Redisplay
Stop Operation
Lookup Certificates on Server
Clipboard
My Certificates
Certificates
Imported Certificates
Imported Certificates
Imported Certificates
Valid Until
Details
Key-ID
OpenPGP
A47488A6
Kleopatra
Select Certificate File
Libraries Documents My Documents certifikat
Search certifikat
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Apps
Libraries
Apps
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
My Data (D:)
Documents library
certifikat
Arrange by: Folder
6EC85A6516C21A5F600B1646242D775EA47488A6.asc
rahasia.asc
File name: rahasia.asc
Certificates (*.asc *.cer *.cert *.c
Open
Cancel
Certificate Import Result – Kleopatra
Detailed results of importing C:\Users\Luki\Documents\certifikat\rahasia.asc:
Total number processed: 1
Imported: 0
Secret keys processed: 1
Secret keys unchanged: 1
OK

12. Selanjutnya Buat pesan yang ingin dienkripsi.

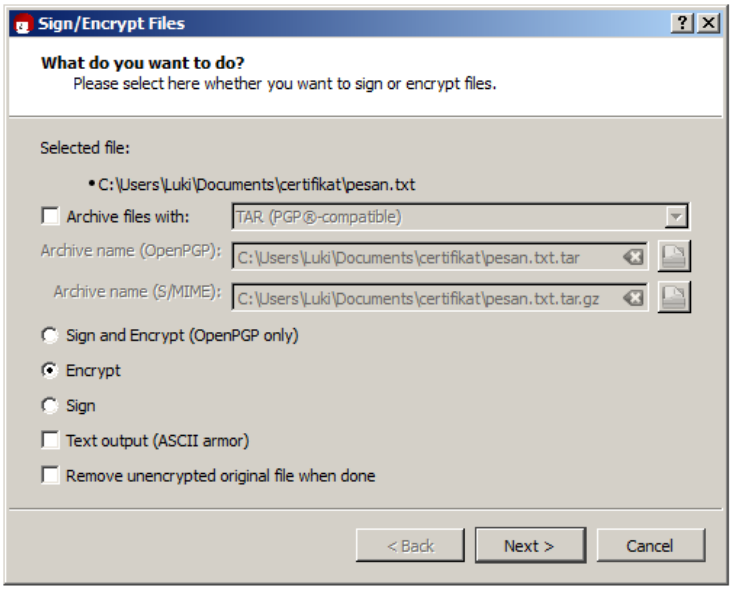


13. Lalu buka File > Encryp File > pilih file yang akan dienkripsi.

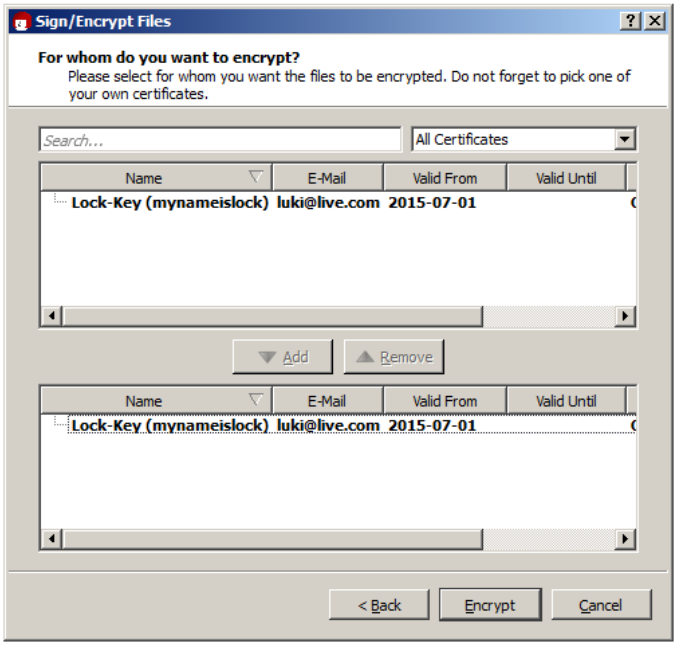


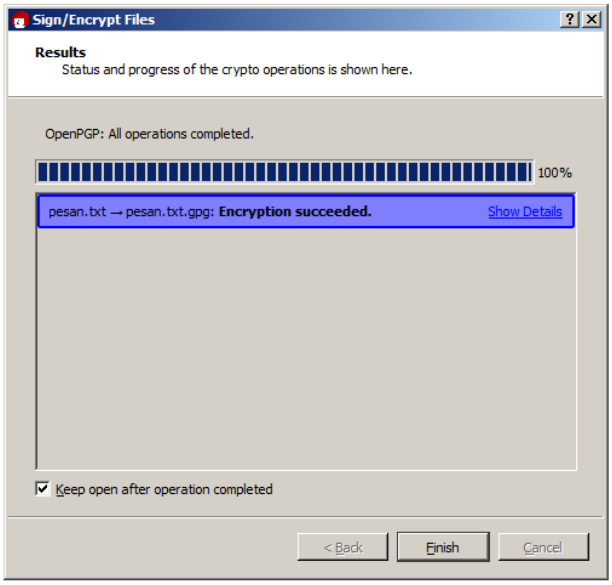


14. Selanjutnya klik next.

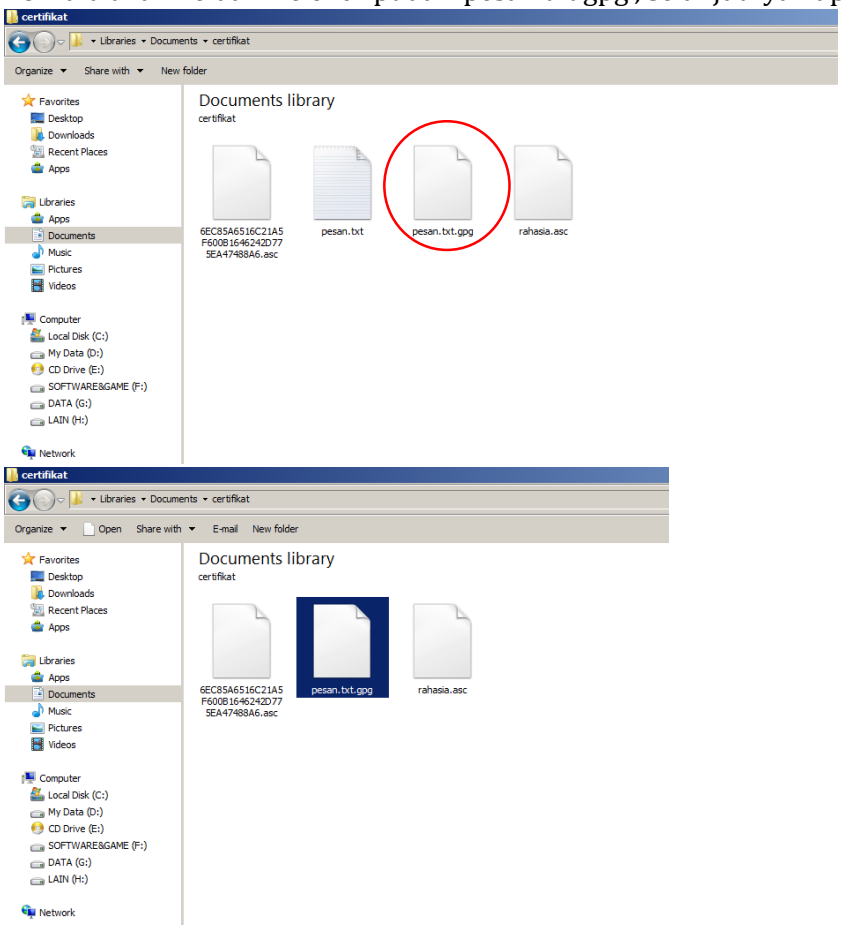


15. Lalu pilih alamat emai tujuan yang telah dibuat, selanjutnya klik add > klik Encrypt > lalu klik finish.

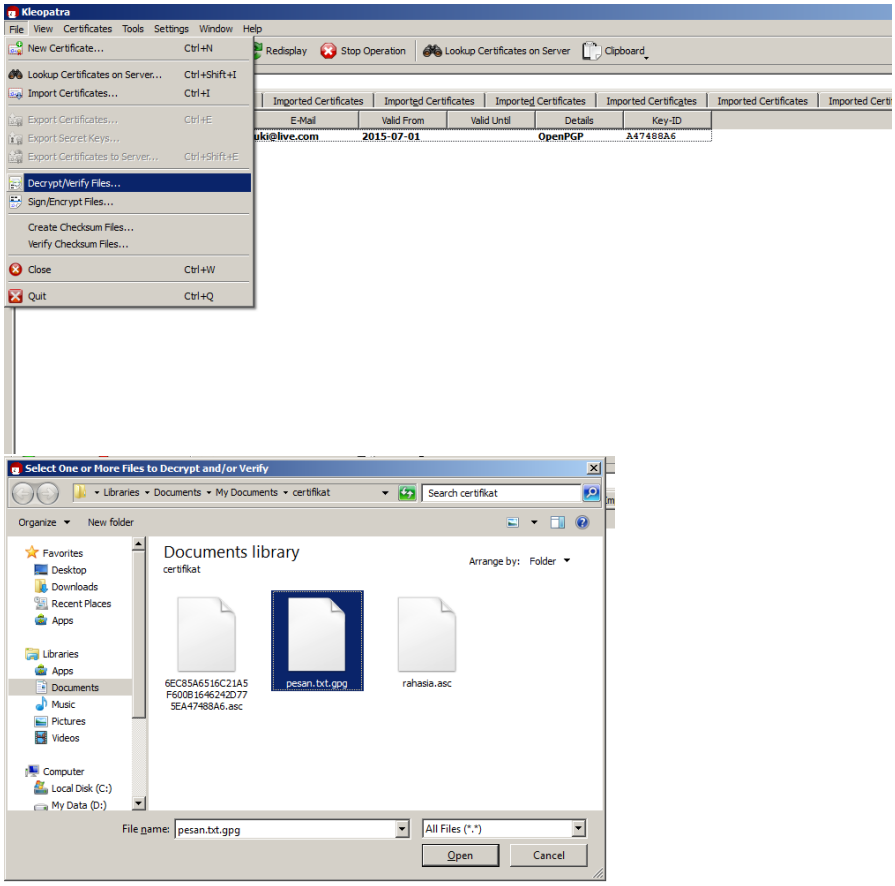




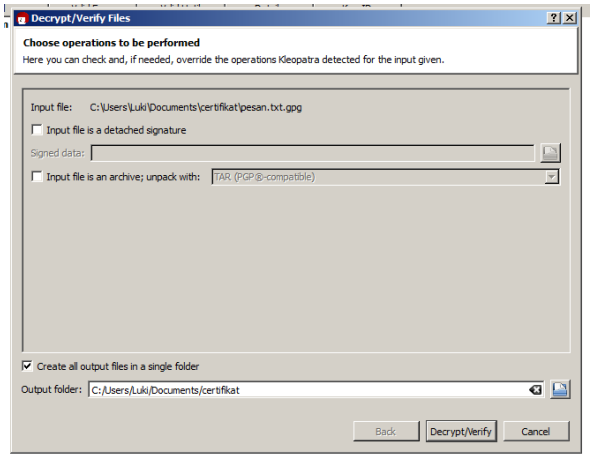
16. Lalu akan keluar file encript dari pesan.txt.gpg , selanjutnya hapus file asli pesan.txt



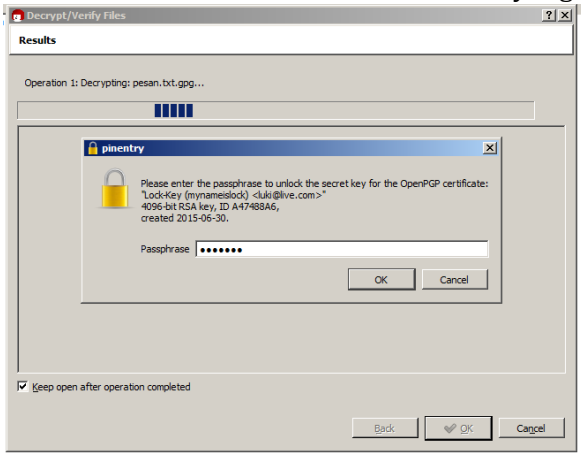
17. Selanjutnya klik file > Decrypt > pilih file pesan.txt.gpg yaitu file hasil encrypt > open



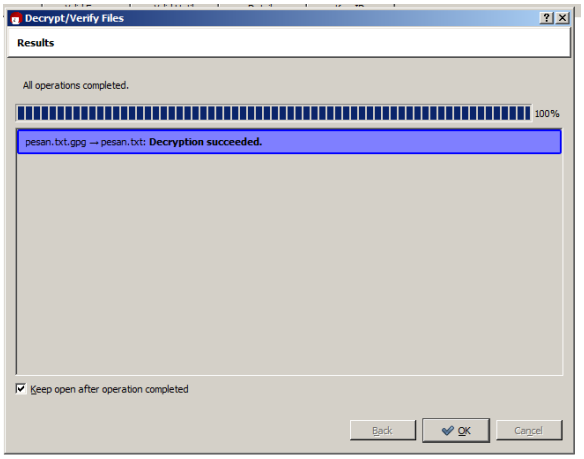
18. Selanjutnya klid Decrypt.



19. Masukkan Password untuk sertifikat yang sudah dibuat.



20. Klik Ok.



21. File telah berhasil di Decrypt dengan pesan plaint text.