Nama : Faizal Rizki Nugroho
Nim : 1310651026
Kelas : A

1. **Certified Information Systems Security Professional (CISSP)**

   Common Body of Knowledge atau CBK dari keamanan sistem informasi menjadi basis dari International Information Systems Security Certification Consortium, atau ISC2 (http://www.isc2.org/). Standar seperti BS17779 dan ISO7799 menjadi dasar dari CBK. Ujiannya dibuat oleh badan testing professional dan selalu di revisi/diperbaharui sesuai perkembangan di industri IT sekuriti. Untuk menjadi seorang Certified Information Systems Security Professional (CISSP), sebelumnya harus lulus ujian yang terdiri dari 250 pertanyaan multiple-choice yang harus diselesaikan dalam waktu 6 (enam) jam! Ujiannya meliputi 10 (sepuluh) dasar dari CBK yaitu:

   - Access Control Systems & Methodology
   - Computer Operations Security
   - **Cryptography**
   - Application & Systems Development
   - Business Continuity & Disaster Recovery Planning
   - Telecommunications & Network Security
   - Security Architecture & Models
   - Physical Security
   - Security Management Practices
   - Law, Investigations & Ethics

   Cryptography (Kriptografi)
   Kriptografi adalah bidang ilmu pengetahuan yang mempelajari pemakaian persamaan matematika untuk melakukan proses penyandian data (Onno, 2000). Kriptografi bertujuan untuk mengaankan isi data atau menjaga kerahasiaan informasi dari orang yang tidak berhak untuk mengetahui isi data tersebut. Dengan teknik atau algoritma tertentu yang disebut proses enkripsi (encypt), data diubah menjadi data sandi yang bentuknya berbeda dengan data aslinya.

   Orang yang berhak menerima data akan mengetahui algoritma dan memiliki kunci untuk mengembalikan data sandi menjadi bentuk data aslinya, proses ini disebut dekripsi (decrypt). Bentuk data sandi diperlukan pada saat proses penyimpanan atau proses pengeriman data. Untuk dapat melakukan proses enkripsi dan deksripsi maka pihak pengirim dan penerima harus mengetahui algoritma kroptografi yang digunakan serta memiliki kunci yang sesuai. Tingkat keamanan dari data sandi terhadap upaya proses dekripsi secara paksa oleh orang yang tidak berhak ditentukan oleh kekuatan algoritma yang digunakan dan kerahasiaan kunci. Kekuatan algoritma yang digunakan untuk proses enkripsi dan dekripsi berhubungan erat dengan penggunaan persamaan matematika. Semakin banyak dan rumit perhitungan dari persamaan matematika yang digunakan maka data sandi semakin aman (Alfred, 1997).

Pemanfaatan kecepatan dan ketelitian dari kerja komputer sangat membatu untuk proses ini. Kerahasiaan kunci adalah bagaimana cara kunci tersebut disimpan dan didistrubusikan kepada pihak yang berhak menerima data, karena kunci ini akan digunakan untuk melakukan dekripsi. Semakin rapi kunci disimpan dan didistribusikan maka data sandi semakin aman.

Pemanfaatan kecepatan dan ketelitian dari kerja komputer sangat membantu untuk proses ini. Kerahasiaan kunci adalah bagaimana cara kunci tersebut disimpan dan didistribusikan kepada pihak yang berhak menerima data, karena kunci ini akan digunakan untuk melakukan dekripsi. Semakin rapi kunci disimpan dan didistribusikan maka data sandi semakin aman. Berikut ini adalah istilah-istilah yang berhubungan erat dengan kriptografi (Onno, 2000).

a. Plaintext / cleartext adalah data asli atau informasi bersifat terbuka yang isinya dapat dibaca dan dipahami secar langsung. Menjadi sumber data untuk proses enkripsi.
b. Chiphertext adalah data sandi hasil proses dekripsi.
c. Cipher adalah algoritma untuk mengubah plaintext menjadi ciphertext menggunakan persamaan matematika. Hasil perubahan dapat berbentuk substitution cipher, transposition cipher, atau gabungan dari keduanya.
d. Substitution cipher adalah algoritma mengubah plaintext menjadi ciphertext dengan cara mengganti menggunakan persamaan matematika tertentu.
e. Transposition cipher adalah algoritma mengubah plaintext menjadi ciphertext dengan cara menggeser menggunakan persamaan matematika tertentu.
f. Block cipher adalah algoritma mengubah plaintext menjadi ciphertext untuk setiap block data. Jumlah data atau besarnya block adalah tertentu.
g. Kunci (key) adalah data atau nilai yang sangat spesifik yang diketahui oleh pengirim dan penerima yang berhak. Digunakan bersama-sama dengan algoritma kriptografi untuk melakukan proses enkripsi dan dekripsi.
h. Enkripsi (encryption) adalah proses yang digunakan untuk menyamarkan/menyembunyikan plaintext. Hasil dari proses enkripsi adalah data sandi (ciphertext).
i. Dekripsi (decrytion) kebalikan dari proses enkripsi yaitu mengembalikan ciphertext menjadi plaintext.
j. Kriptosistem (cryptosystem) adalah sistem kriptografi yang ddidalamnya terdiri dari: algoritma kriptografi, plaintext, ciphertext, key, dan unsur lain yang berpengaruh dalam sistem kriptografi.
k. Cryptanalysis / code breaking adalah kegiatan untuk mengubah ciphertext menjadi pesan aslinya tanpa mengetahui kunci yang sesuai, dengan coba-coba (trial and error) secara sistematis.
l. Cryptology adalah ilmu matematika yang mendasari crythography dan cryptanalysis.

Cakupan Kriptografi :

– kriptografi simetrik
– kekuatan kunci
– PKI: Public Key Infrastruktur
– fungsi hash
– serangan kriptografi
– kriptografi asimetrik
– system kriptografi
– fungsi satu arah
– pengelolaan kunci
– tandatangan digital.

Ilustrasi fungsi password (satu arah)

passwd user1
Enter new UNIX password: [rahasia]
Retype new UNIX password: [rahasia]

Ilustrasi berkas /etc/shadow

...
user1:1ADaQTYGz$xjHux3HCLvq.zw3Yq1Sit.:13115:0:99999:7:::
...

Ilustrasi Membuat Kunci GnuPG

gpg --gen-key
[...]
gpg: /home/dummy/.gnupg/trustdb.gpg: trustdb created
gpg: key A8F128EE marked as ultimately trusted
public and secret key created and signed.
[...]
pub 1024D/A8F128EE 2005-11-29
Key fingerprint = D8F8 D13D 3CBC 6990 FF47 5B15 7873 7940 A8F1 28EE
uid Dummy <dummy@dummy.com>
sub 2048g/8BEEDC59 2005-11-29

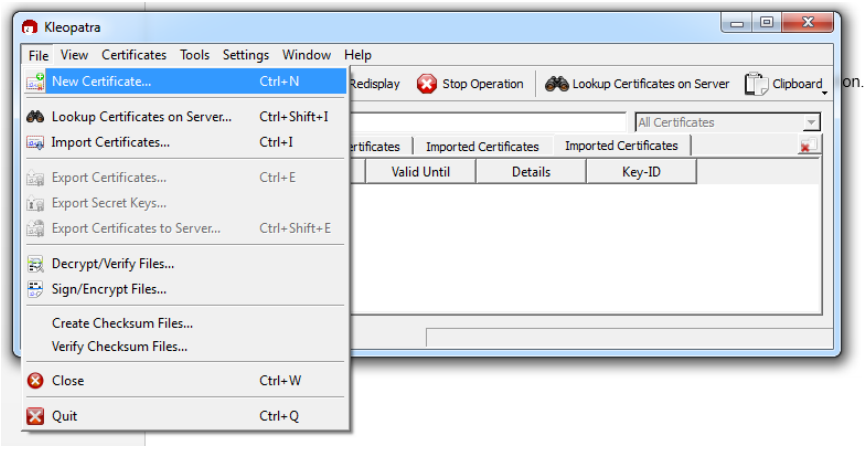
Tanda-tangan berkas "Release" dengan GnuPG

gpg -b --armor -o Release.gpg Release

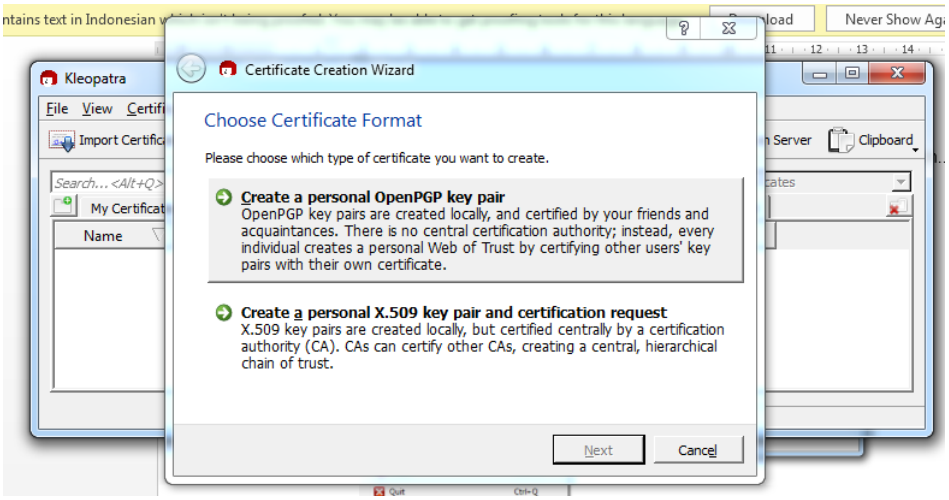
Berikut adalah contoh metode Caesar Cipher.
Plaintext: "ABCDEFGHIJKLMNOPQRSTUVWXYZ",
digeser dengan urutan 3 huruf didepannya menjadi :
Ciphertext: "DEFGHIJKLMNOPQRSTUVWXYZABC"
Ciphertext tersebut digunakan untuk mengubah
Plaintext: "SEMARANG KOTA ATLAS", di peroleh hasil Ciphertext sebagai berikut : "VHPDUDQK NRWD
DWODV"

2. Saya menggunakan GPG4win untuk melakukan pengiriman e-mail encryption..

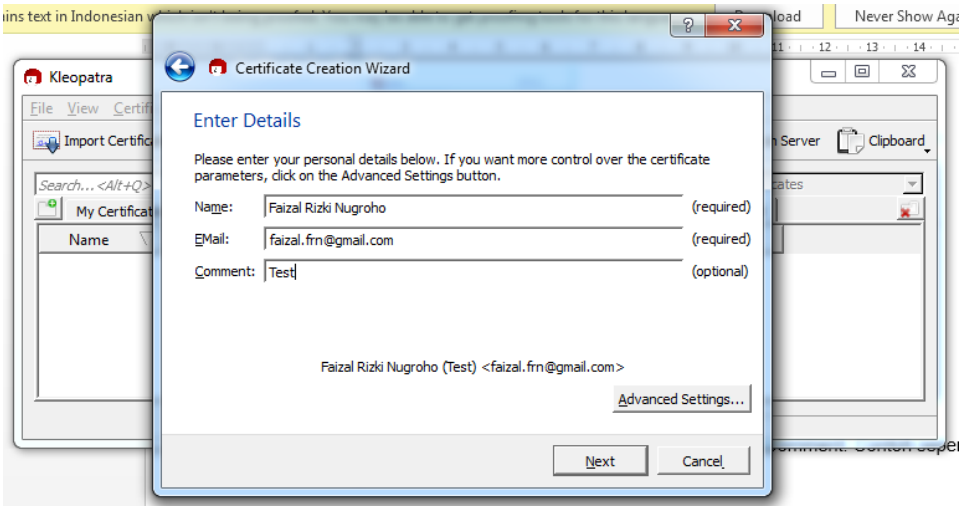
- Step 1 buka software **Kleopatra,** pilih File kemudian

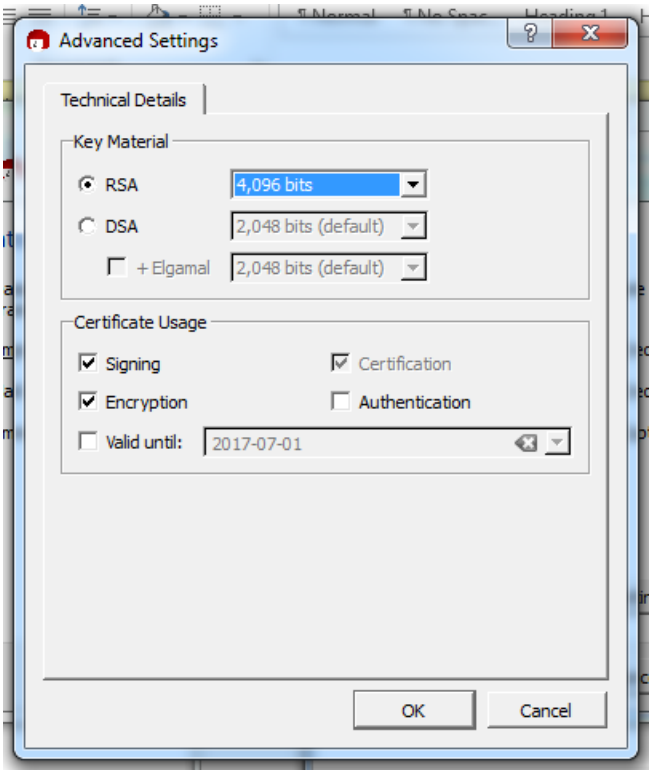


- Step 2 pilih **Create a personal OpenGPG key pair** klik Next

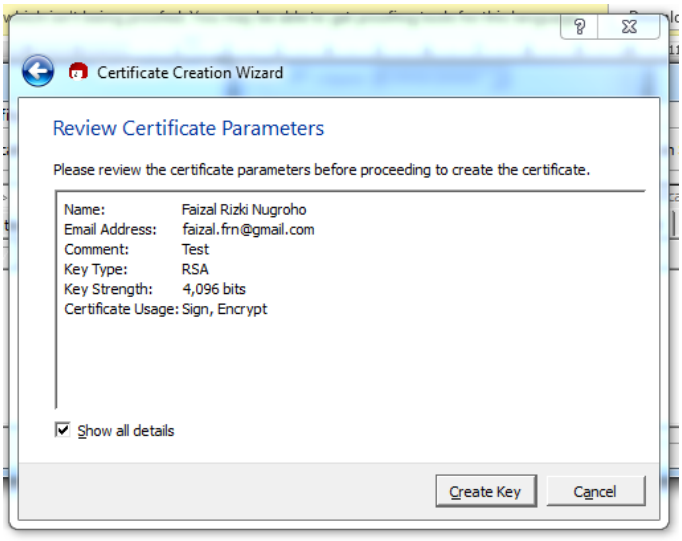


- Step 3 disitu kita harus mengisi Name, e-mail, dan Comment. Contoh seperti gambar dibawah, jangan lupa Advanced Settings **RSA 4,096** bits seperti dibawah, kemudian klik Next:

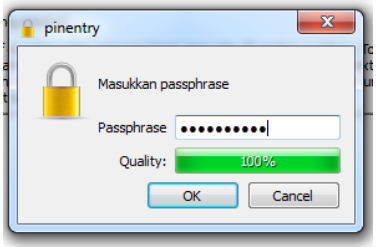


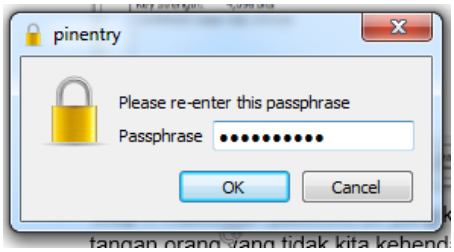


- Step 4 berikutnya akan tampil seperti dibawah, centang Show all details klik Create Key

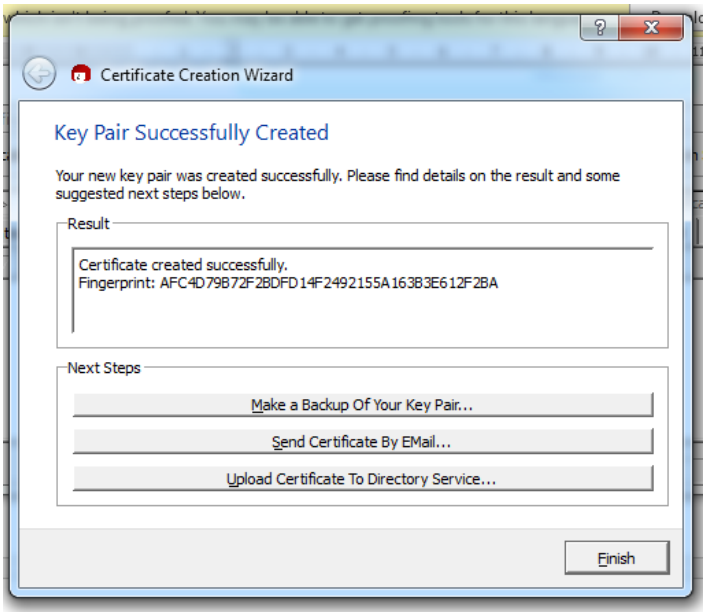


- Step 5 masukkan pasword 2x yang kita inginkan, guna jika pesan kita jatuh ke tangan orang yang tidak kita kehendaki tetap aman

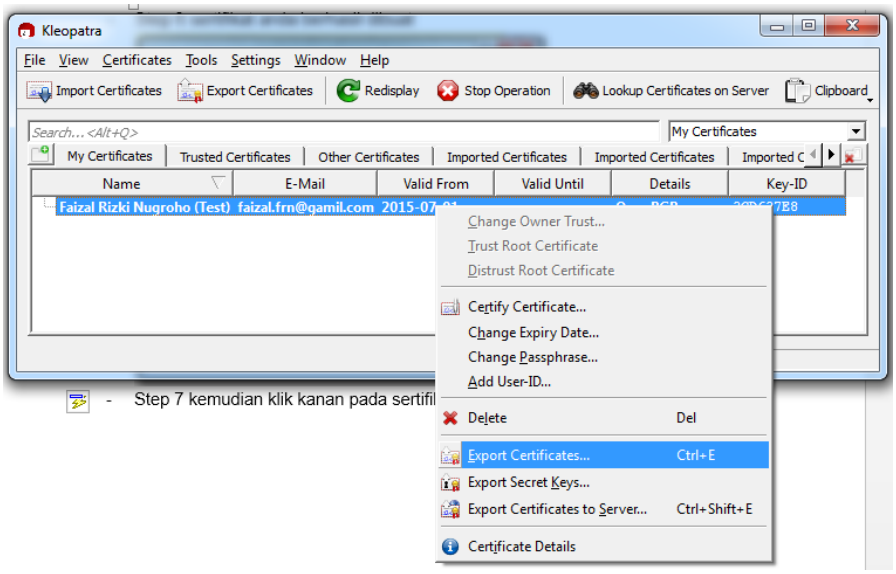




- Step 6 sertifikat anda berhasil dibuat

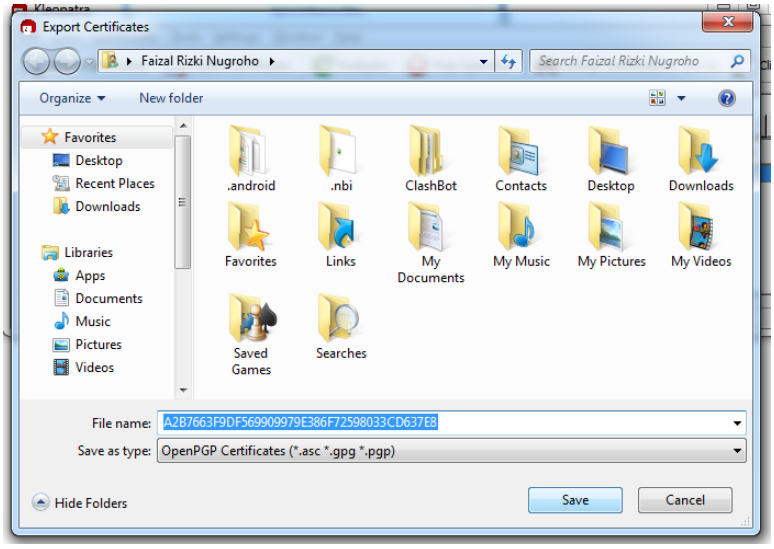


- Step 7 kemudian klik kanan pada sertifikat yang kita buat pilih Export Certificates

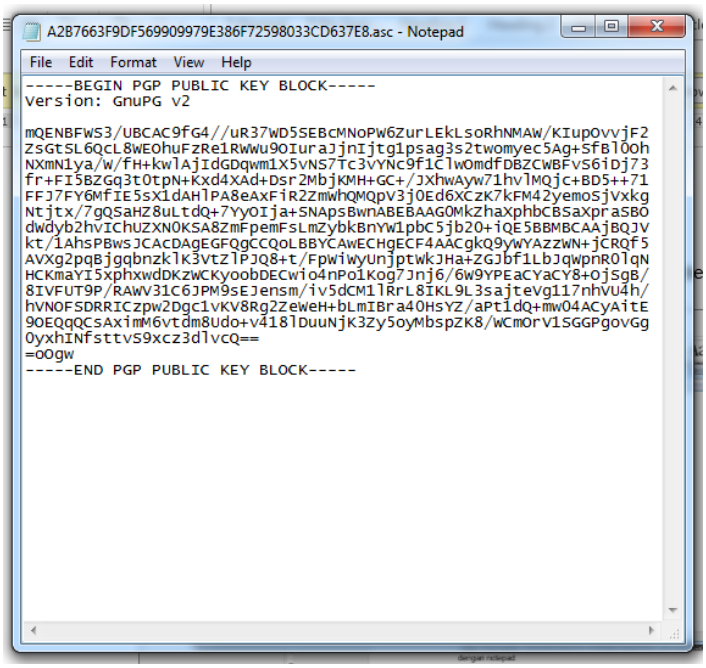


- Step 7 kemudian klik kanan pada sertifi

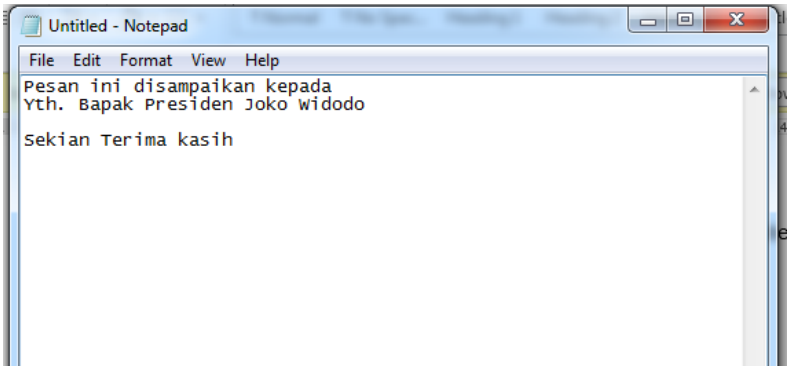
- Step 8 pilih tempat untuk menyimpan, klik Save



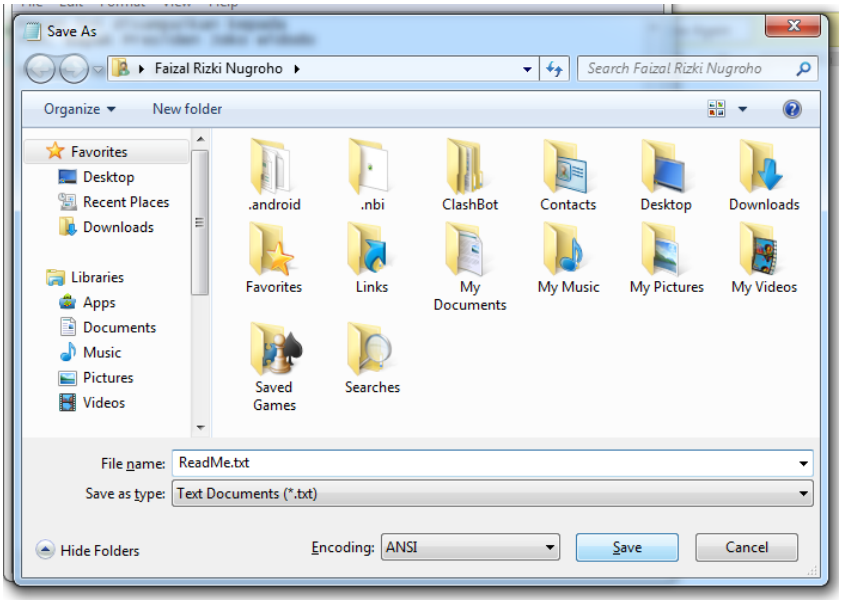
- Step 9 kemudian coba kita buka file Sertifikat yang telah kita save sebelumnya dengan notepad



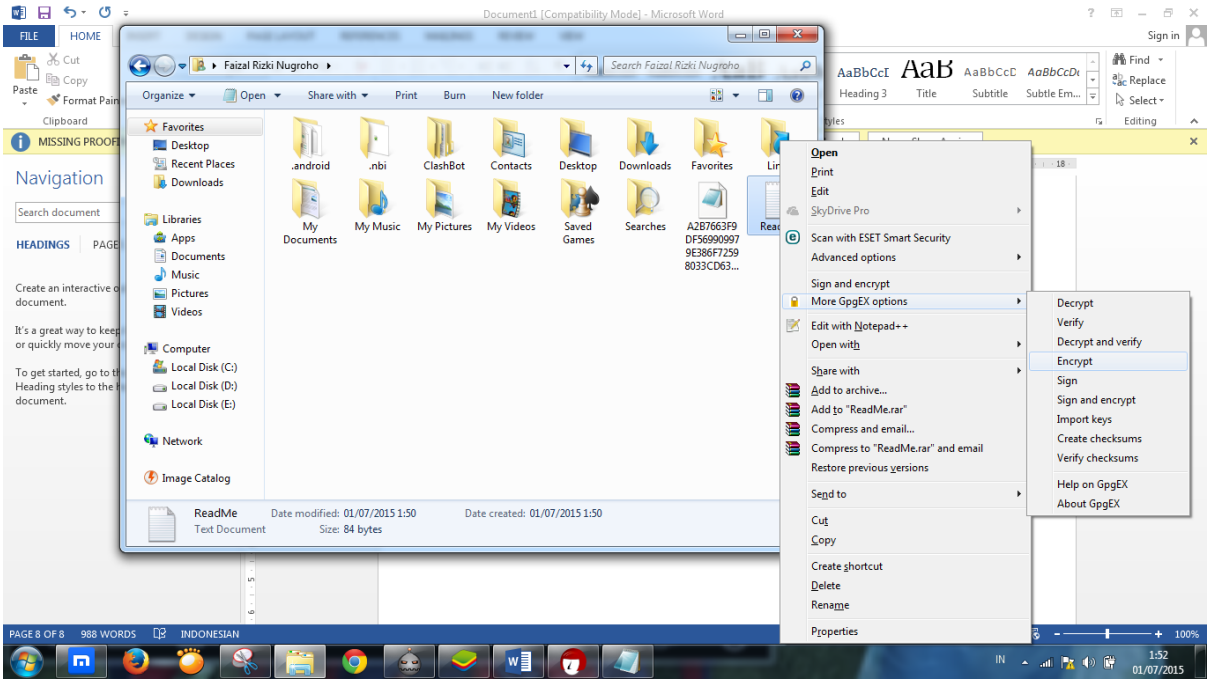
- Step 10 sekarang coba kita buat file txt, tulis apa yang ingin kita jadikan pesan enkripsi, contoh seperti gambar dibawah ini



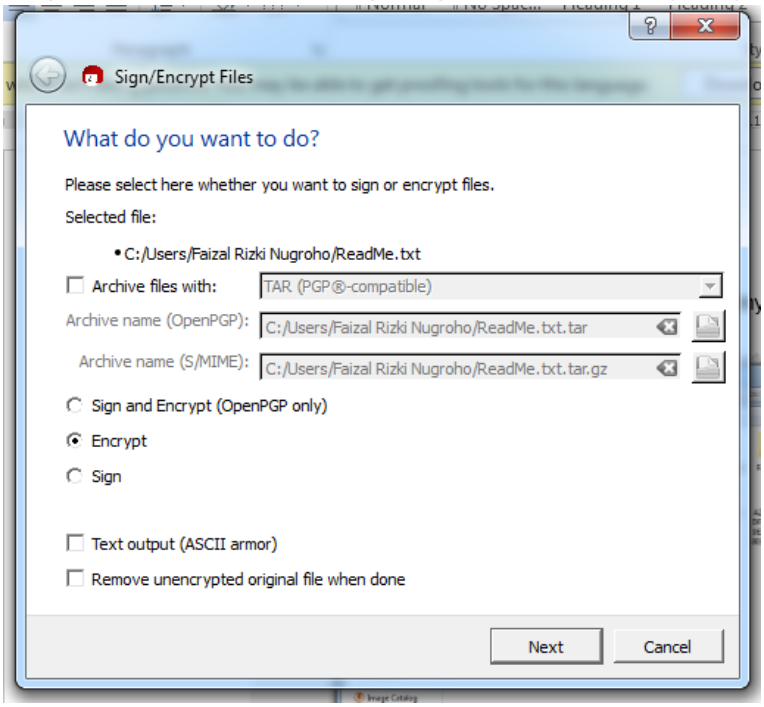
- Step 11 simpan ke tempat yang kita inginkan beri nama dengan type file txt



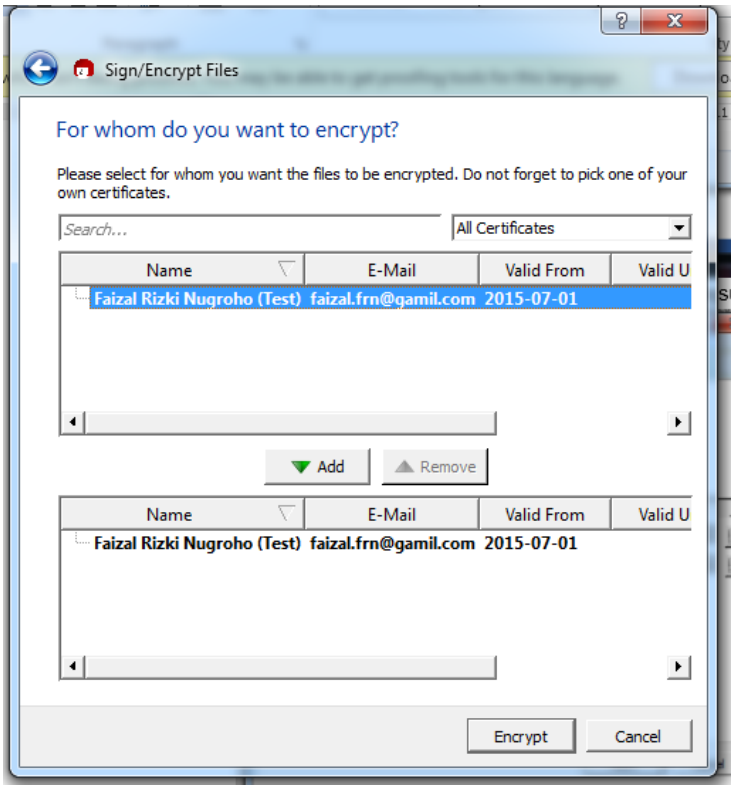
- Step 12 klik kanan pada file yang kita buat sebelumnya, pilih More GpgEX options pilih Encrypt



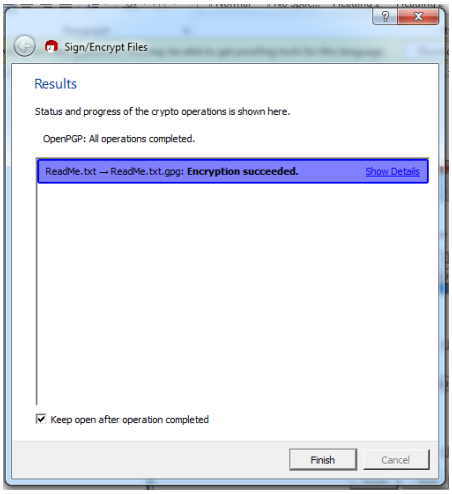
- Step 13 kemudian akan tampil seperti dibawah, langsung klik Next



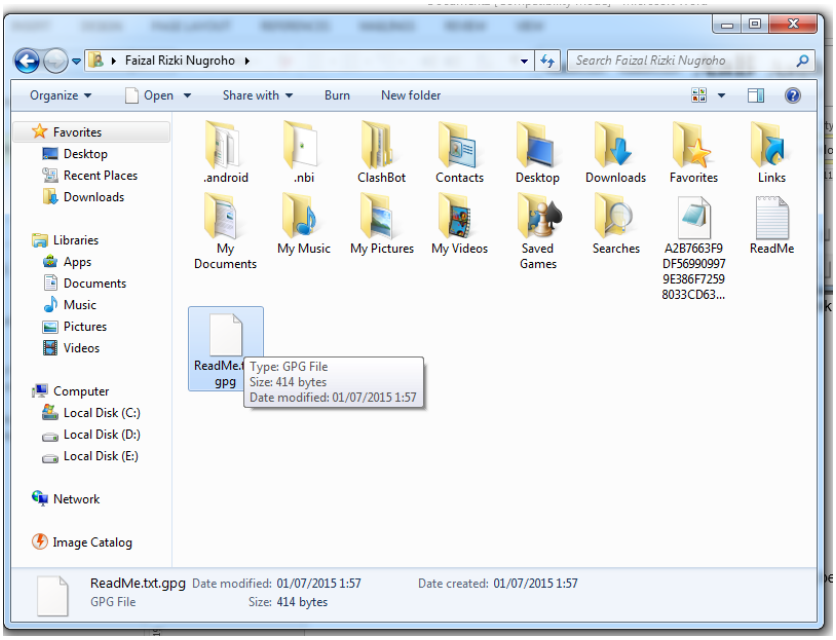
- Step 14 kemudian pilih sertifikat kita yang telah kita buat tadi, klik Add kemudian klik Encrypt



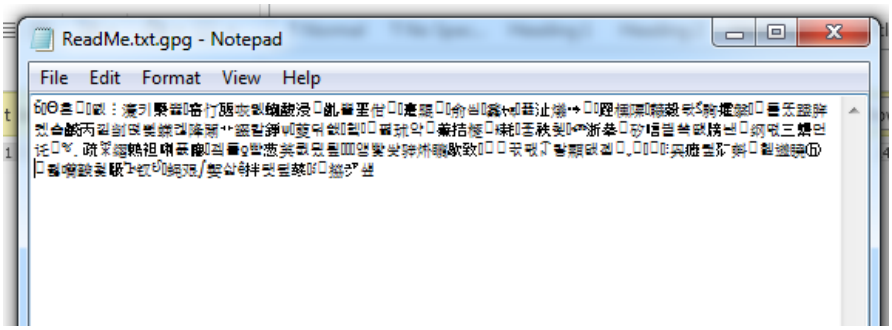
- Step 15 tunggu hingga tampil seperti dibawah ini, klik Finish



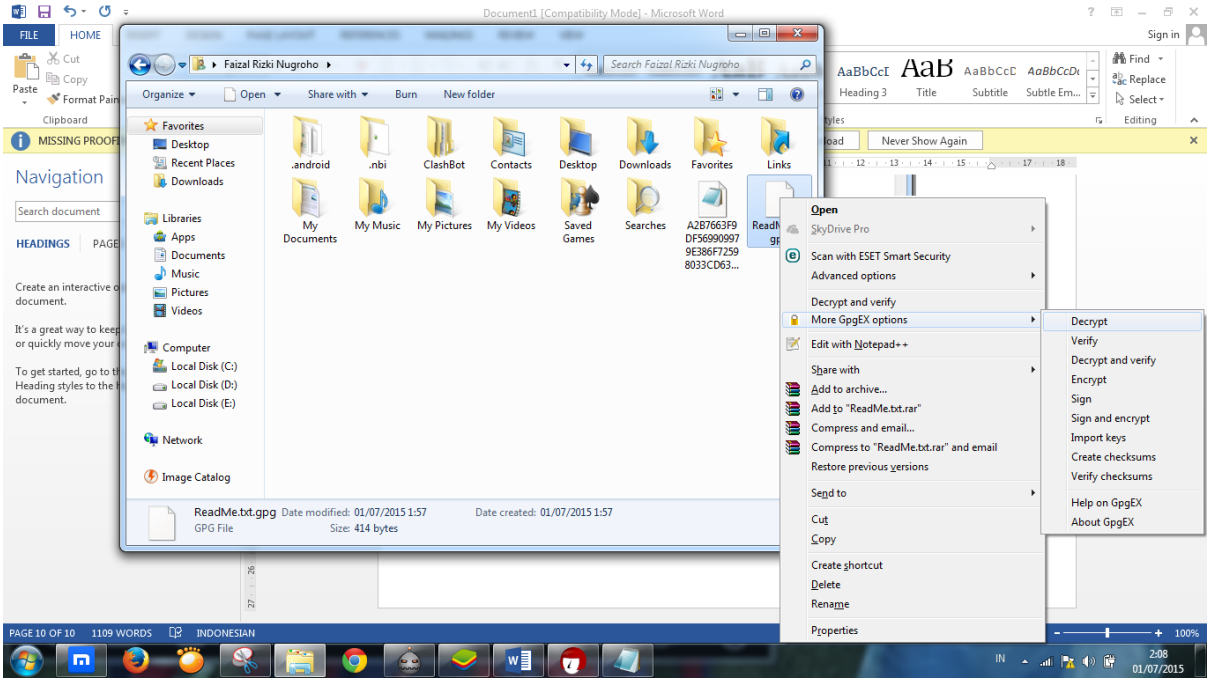
- Step 16 maka akan otomatis muncul file baru yang berformat .gpg



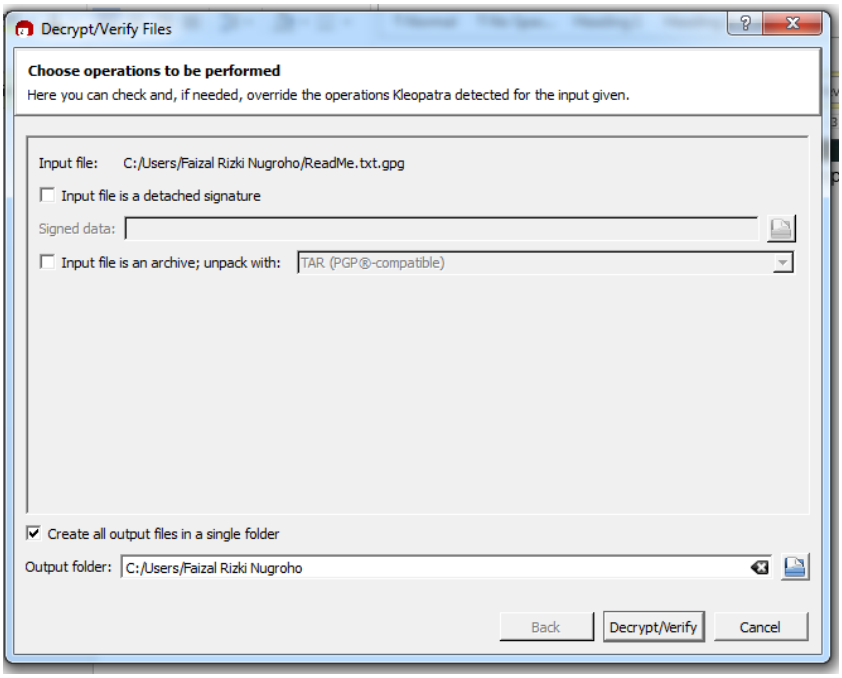
- Step 17 coba kita lihat menggunakan notepad, akan tampil seperti dibawah ini. Disini pesan yang kita kirimkan tidak akan terbaca pesan aslinya oleh pihak ketiga.



- Step 18 jika kita sebagai penerima pesan dan ingin mengetahui apa isi pesan tersebut hampir sama dengan yang diatas cuman kita menggunakan Descrypt. Sebelumnya coba kita hapus file ReadMe.txt tadi, kemudian buka file ReadMe.txt.gpg dengan klik kanan, pilih More GpgEX options pilih Descrypt

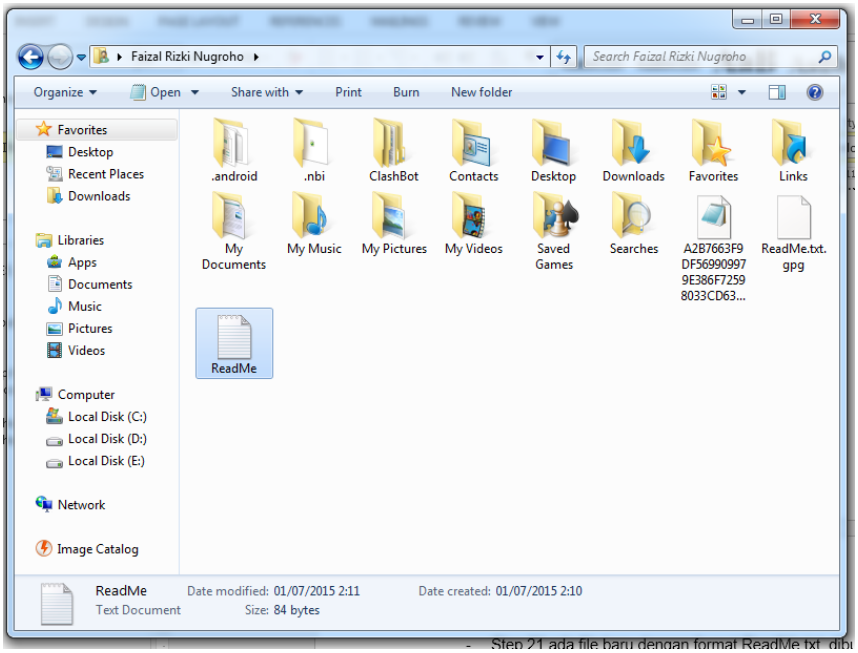


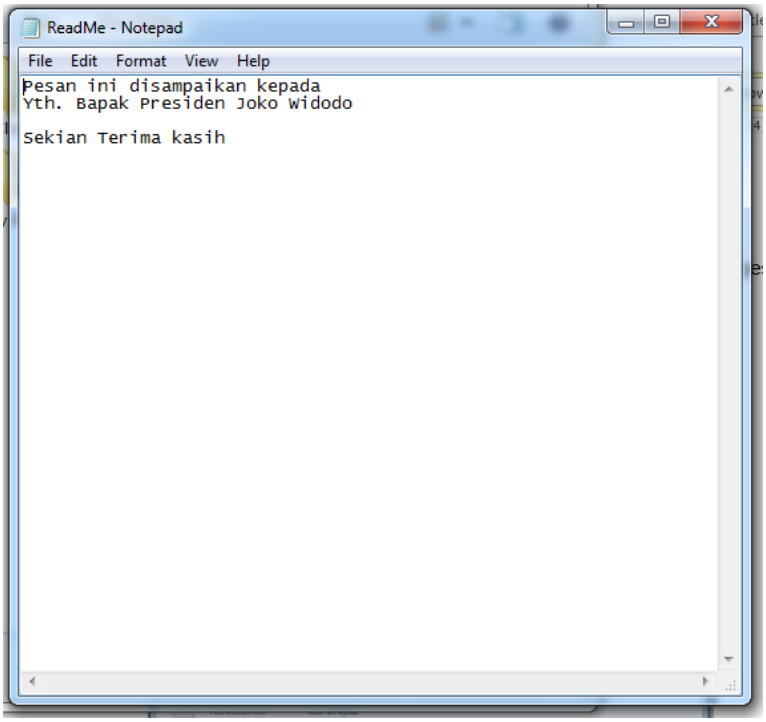
- Step 19 akan tampil pemberitahuan seperti dibawah, klik Descrypt/Verify



- Step 20 dan kita akan dimintai password yang telah kita buat saat membuat sertifikat di awal tadi

- Step 21 ada file baru dengan format ReadMe.txt, dibuka dan terlihat pesan yang tadi terenkripsi





- Selesai