***Pair Key (Private and Public) Encryption***

**Sistem Operasi Genap 2016/2017**

**Fakultas Ilmu Komputer – Universitas Indonesia**

Oleh : Ibad Rahadian Saladdin (1406623695)

* **Pendahuluan**

Pada dunia IT, transmisi file dari satu orang ke orang lainnya merupakan hal yang biasa. File ini nantinya dapat digunakan untuk banyak keperluan, seperti kolaborasi untuk mengembangkan suatu program. Tetapi jika file yang ingin di-transmisikan jatuh ke tangan orang yang salah dan tidak bertanggung jawab, maka dapat menimbulkan banyak masalah seperti plagiarism atau kebocoran data karena, terkadang dari file-file tersebut juga memiliki informasi-informasi yang sensitif yang tidak dapat dilihat oleh semua orang.

Maka dari itu, perlu dibuat suatu pengaman agar informasi-informasi yang ada pada sebuah *file* tidak mudah hilang ataupun dicuri oleh orang lain. Cara yang mudah adalah dengan OpenPGP Pair Key, dengan menggunakan *public* dan *private key*. *Public key,* dimana kunci ini tersebar dan dapat diakses oleh semua orang. Sedangkan, *private key* hanya dapat diakses oleh pembuat *key* tersebut. Enkripsi jenis ini memungkinkan kita secara langsung menentukan tujuan siapa yang dapat membuka enkripsi ini sehingga pihak-pihak lain yang tidak diberikan akses tidak dapat melihat file tersebut.

Berikut adalah panduan untuk melakukan enkripsi OpenPGP dengan menggunakan Windows (Kleopatra) dan juga Linux.

Pada panduan ini, digunakan **GitHub** sebagai repository untuk memudahkan transfer file antar pengguna. Disarankan bagi pengguna Windows untuk meng-*install tools* Kleopatra dan GitHub Client for Windows. Sedangkan bagi pengguna Linux untuk meng-*install* git dengan melakukan ini pada terminal Anda :

sudo apt-get update

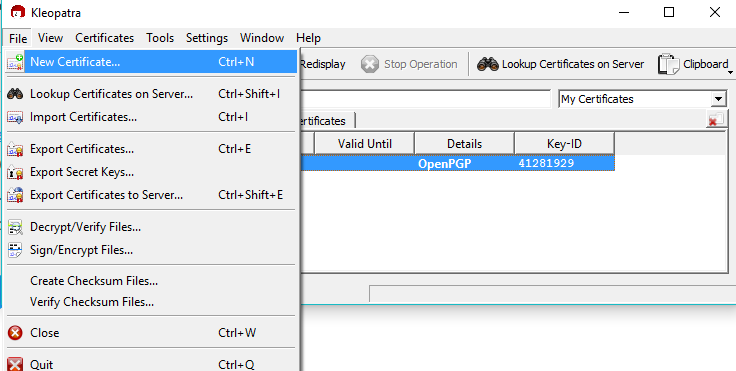
sudo apt-get install git

* **Membuat Key**

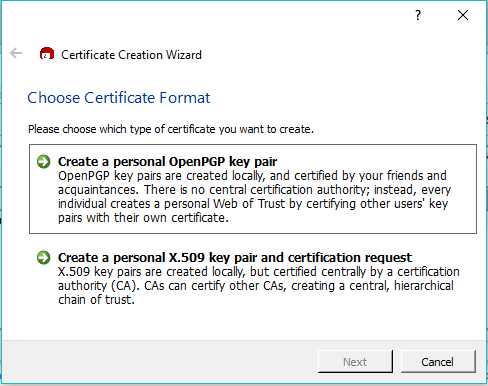
1. **Windows (Menggunakan Kleopatra)**

**Tips :** Silahkan unduh pada halaman berikut <https://www.gpg4win.org/features.html>

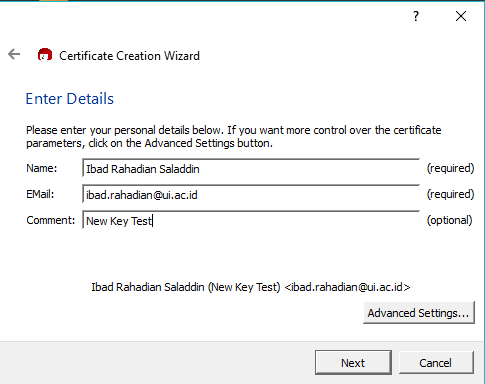
* 1. Buka menu membuat key baru dengan *File -> New Certificate*.



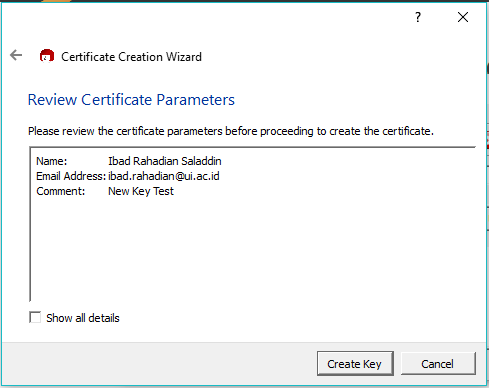
* 1. Pilih menu “*Create a Personal OpenPGP Pair*”



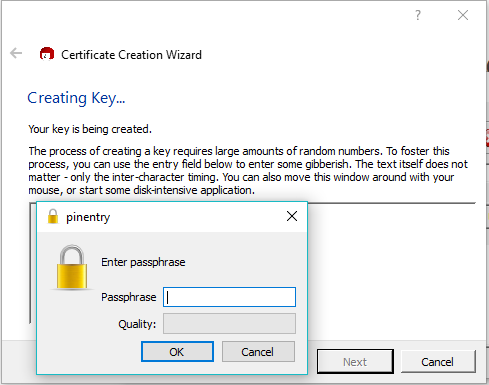
* 1. Masukkan detil data diri Anda.



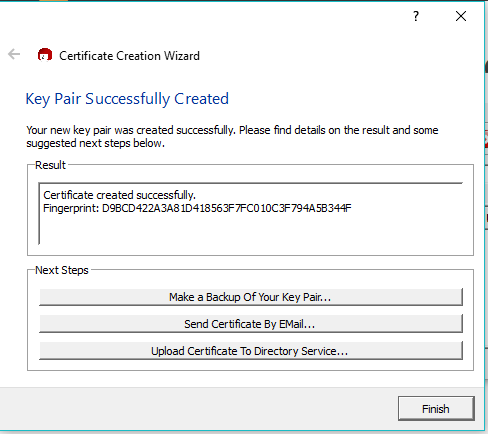
* 1. Silahkan review data yang sudah Anda masukkan, tekan *Next*.



* 1. Masukkan kata kunci Anda, jangan beritahukan kepada orang lain sebanyak dua kali.



* 1. Tekan *Finish*.



1. **Linux**

**Tips :** Semua operasi di Linux pada tutorial ini menggunakan *Command Line.* Jadi harus menggunakan Terminal.

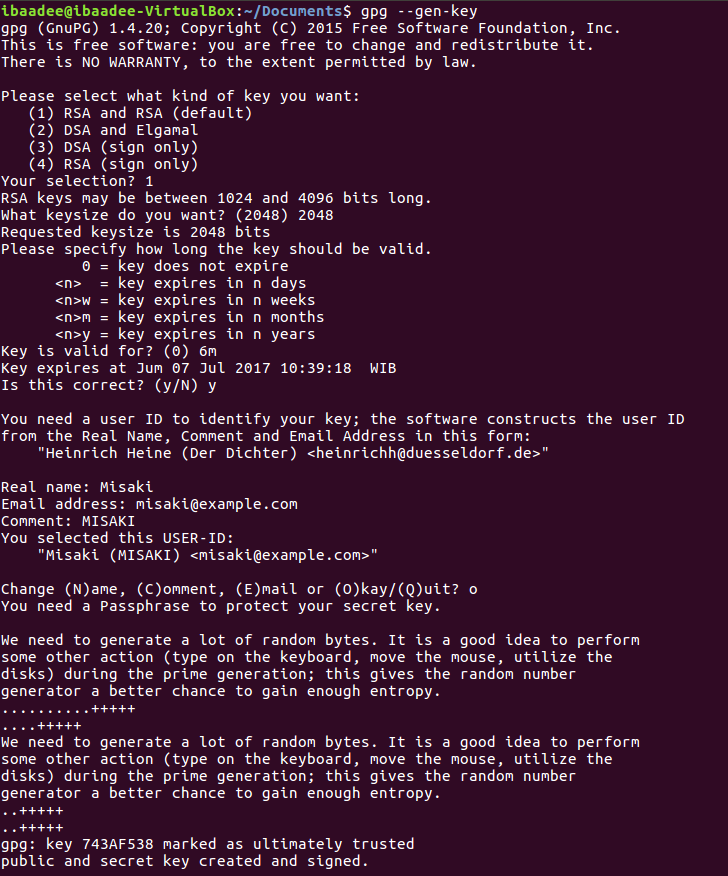
* 1. Inisiasi pembuatan key baru dengan gpg –-gen-key
  2. Pilih menu “RSA and RSA (default)”dengan menekan ‘1’ lalu Enter.
  3. Masukkan jumlah bit yang diinginkan dengan ‘2048’ (default) atau sesuai dengan yang Anda inginkan.
  4. Masukkan berapa lama key ini berlaku, e.g ‘6m’ untuk waktu 6 bulan atau sesuai dengan yang Anda inginkan.
  5. Masukkan identitas anda (Nama, e-mail, dan *Comment*).
  6. Masukkan *passphrase* Anda.
  7. Cek apakah key sudah masuk dengan gpg --list-keys.
  8. Jika sudah ada, berarti key sudah selesai dibuat.

Dibawah ini terdapat ilustrasi yang telah dijalankan pada sistem Ubuntu.

**Tips Menyimpan *Passphrase* agar tidak lupa**

*Passphrase* pada enkripsi jenis ini penting untuk diingat, karena tidak ada mode lupa kata sandi agar tidak mudah untuk ditembus oleh orang lain. Langkah antistipatif yang dapat diambil adalah dengan membuat *hint* pada kata sandi atau cara-cara mudah agar kata sandi selalu diingat.

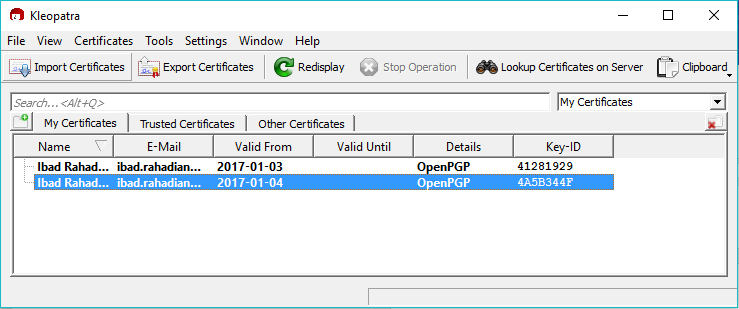
1. Tulislah *hint* kata sandi pada *notes* Anda di tempat yang aman, saya menyarankan menggunakan layanan Google Keep yang dapat diakses dari *mobile* dan web.
2. Buatlah *hint* yang unik, yang sangat internal sehingga orang-orang lain tidak mengetahui maksud yang Anda tulis.
3. Jangan tuliskan kata sandi Anda secara gamblang pada *notes* tersebut.



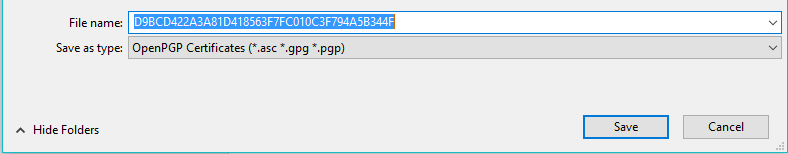
* **Export Key**

**Tips :** Export Key ini digunakan untuk pengguna lain dapat memberikan enkripsi filenya dan dapat dibuka dengan menggunakan key yang Anda berikan. Sertakan key Anda pada setiap pengiriman agar pengguna lain dapat memberikan akses kepada Anda.

1. **Windows (Menggunakan Kleopatra)**
   1. Buka Kleopatra, lalu pilih key yang ingin di-export.



* 1. Klik “Export Certificate”, lalu save dengan nama yang diinginkan.



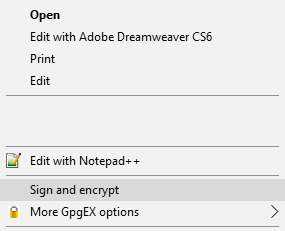
1. **Linux**
   1. Arahkan ke folder tempat key ini nantinya akan disimpan.
   2. Ketik di terminal gpg --armor --export [youremail@example.com](mailto:youremail@example.com) > mykey.asc. “mykey.asc” merupakan nama file yang menyimpan key Anda dan dapat diberi nama sesuai dengan keinginan Anda.
   3. Key sudah siap untuk digunakan.

* **Import Key**

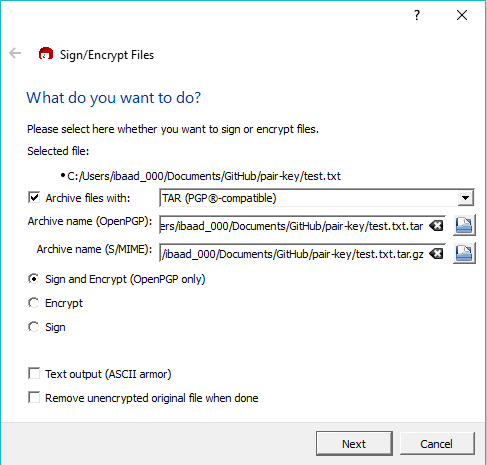
1. **Windows**
2. Buka Kleopatra, lalu pilih menu “Import Certificate”
3. Arahkan ke *directory* penyimpanan key tersebut dengan ekstensi .txt, .asc, .gpg, .pgp
4. Lihat di Kleopatra apakah key sudah masuk.
5. Jika sudah ada, berarti key sudah berhasil di-import.
6. **Linux**
   1. Arahkan kepada *directory* dimana key Anda disimpan.
   2. Jalankan gpg --import mykey.asc. “mykey.asc” dapat diisi dengan nama key Anda.
   3. Cek dengan gpg –list-keys untuk mengecek keberadaan key yang baru saja di-import.
   4. Jika sudah ada, berarti key sudah berhasil di-import.

* **Melakukan Enkripsi**

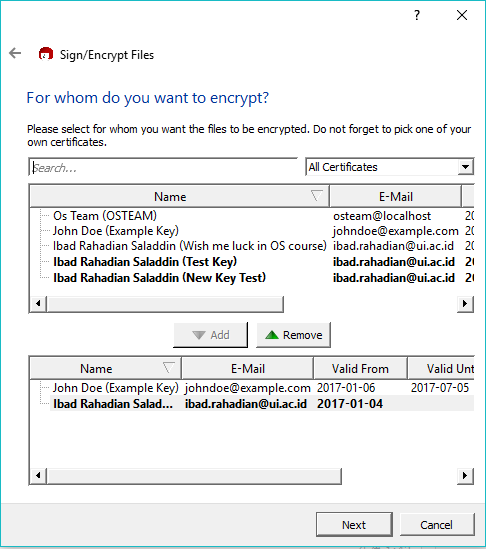
1. **Windows**
2. Klik kanan pada file yang ingin di-enkripsi, lalu tekan *Sign and encrypt*

****

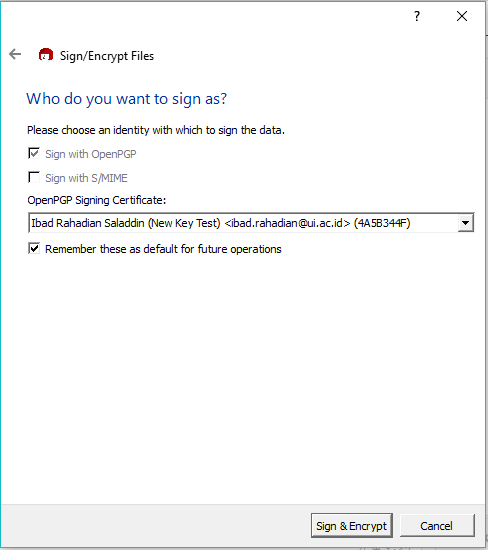
1. Isi tujuan dan *Radio Button “Sign and Encrypt (Open PGP only)* seperti pada gambar dibawah ini.



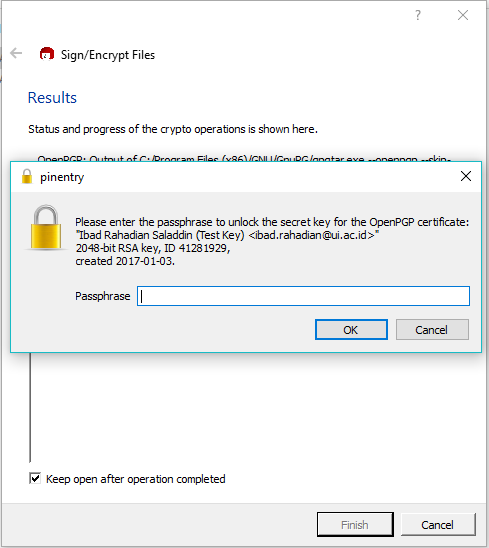
1. Pilih *public key* user yang ingin dituju (termasuk diri sendiri) dengan me-klik tombol *Add.*



1. Masukkan key sebagai pembuat enkripsi dengan memilih salah satu key.



1. Masukkan *passphrase* yang dibuat ketika membuat *key.*



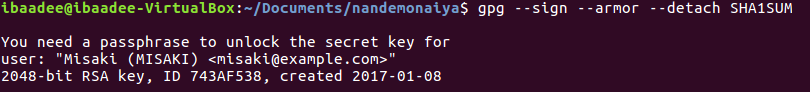
1. Silahkan tekan *Finish. File* telah ter-enkripsi.
2. **Linux**

**Tips :** Melakukan sign dan encrypt pada linux.

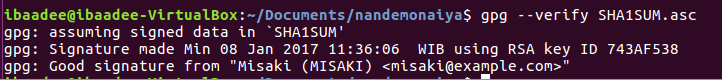
1. Arahkan menuju folder dengan file yang ingin di-enkripsi.
2. Buat kode hash dengan menggunakan sha1sum dengan menjalankan sha1sum \* > SHA1SUM.
3. Jalankan pengecekan sign dengan sha1sum -c SHA1SUM.



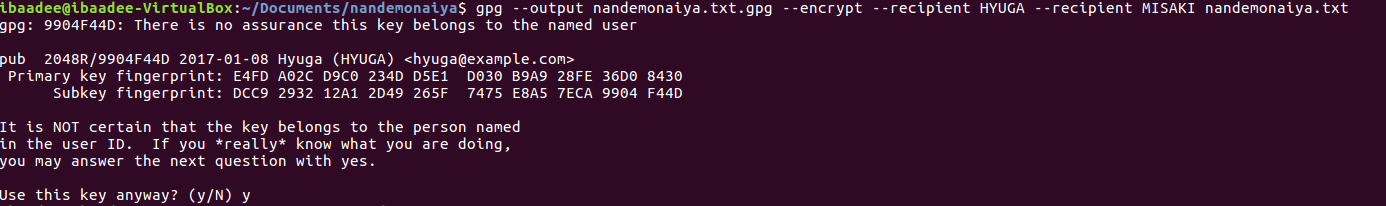
1. Melakukan sign untuk file yang akan di-*encrypt* dengan gpg --sign --armor --detach SHA1SUM. Sign ini digunakan agar pengguna lain mengetahui kalo file ini hasil kerja Anda.



1. Lakukan verifikasi sign Anda dengan gpg –verify SHA1SUM.asc.



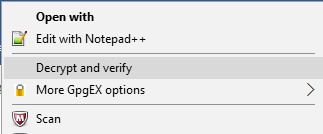
1. Sekarang kita akan melakukan encrypt pada file yang kita inginkan dengan gpg –output nandemonaiya.txt.gpg –encrypt –recipient HYUGA –recipient MISAKI nandemonaiya.txt. Setelah output, merupakan nama file target yang ingin Anda buat beserta dengan ekstensi .gpg yang merupakan file yang telah **ter-enkripsi**. Sedangkan recipient merupakan kepada siapa Anda akan memberikan akses file ini dan jangan lupa untuk **membuat recipent** **dengan key Anda sendiri.**



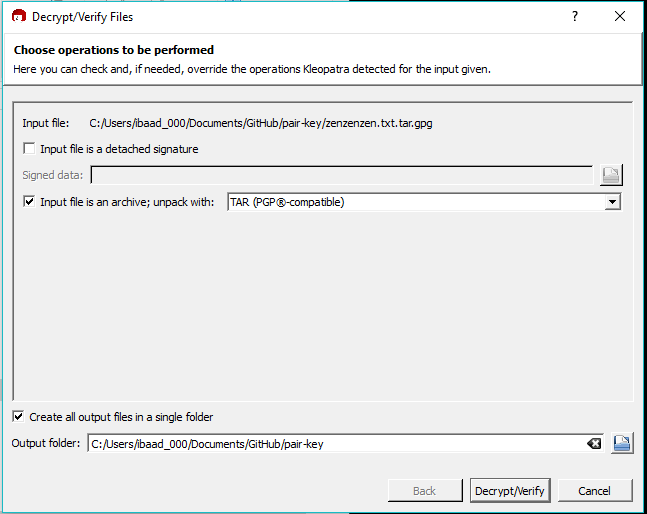
1. Jika file.gpg sudah ada, maka file sudah berhasil ter-enkripsi. Ketika Anda memberikan file ke tujuan Anda, pastikan Anda **menyertakan *public* *key* Anda.**

* **Melakukan Dekripsi**

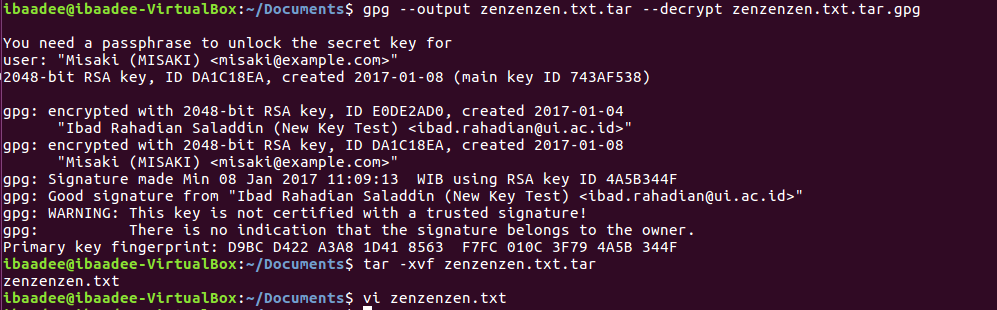
1. **Windows**
2. Klik kanan pada file yang ingin di-dekripsi, lalu klik *Decrypt and verify.*

****

1. Jika *file* yang ingin di-dekripsi menggunakan kompresi .tar, maka centang *check box “Input file is an archive; unpack with: “* dan pilih TAR(PGP®-compatible). Jika tidak menggunakan kompresi maka abaikan saja.

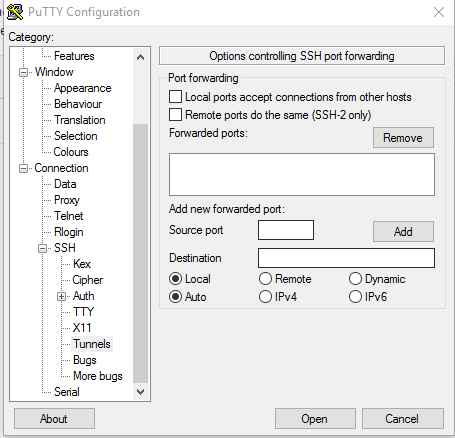


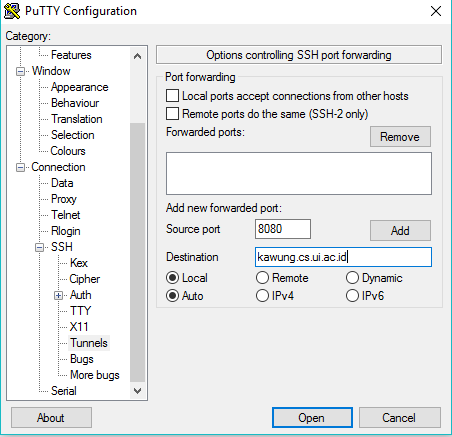
1. Klik *Decrypt/Verify.*
2. Masukkan *passphrase* yang dibuat pada awal pembuatan key.
3. Klik *Finish.*
4. **Linux**
5. Arahkan menuju folder yang mengandung file yang ingin anda dekripsi. Pastikan Anda sudah melakukan import ***public key* dari pembuat file tersebut.**
6. Lakukan dekripsi pada file berekstensi .gpg dengan menjalankan gpg --output zenzenzen.txt.tar --decrypt zenzenzen.txt.tar.gpg. Setelah output merupakan nama target file setelah di-decrypt, disarankan menggunakan **nama yang sama** dengan hanya menghilangkan **ekstensi .gpg** saja.

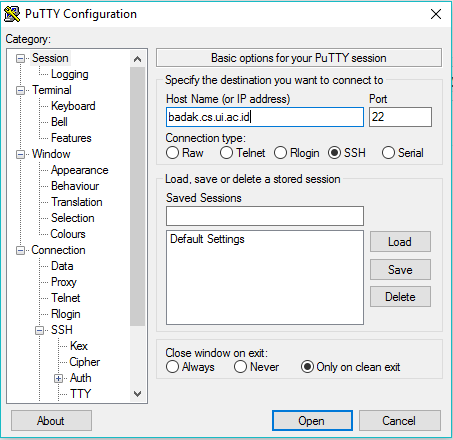


1. **Langkah ini hanya dijalankan jika file masih dikompresi, e.g ber-ekstensi .tar.** Untuk melakukan dekompresi, maka dijalankan tar -xvf zenzenzen.txt.tar. Jika tidak memiliki kompresi, file dapat langsung dijalankan.
2. Akan muncul hasil ekstrak dari kompresi. File ini sudah selesai di-*decrypt* dan dapat dijalankan.

* **Membuat Tunneling ke badak.cs.ui.ac.id**

1. Buka aplikasi PuTTY
2. Pada kotak di sebelah kiri arahkan kepada halaman Connections -> SSH -> Tunnels, lalu masukkan port yang diinginkan dan nama server kawung.cs.ui.ac.id. Lalu, klik tombol *add.*



1. Lalu pada halaman login, lakukan akses ke halaman badak.cs.ui.ac.id, lalu klik *open*. 
2. Lakukan login dengan menggunakan akun LDAP UI Anda.

