

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 plagiarisme 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.

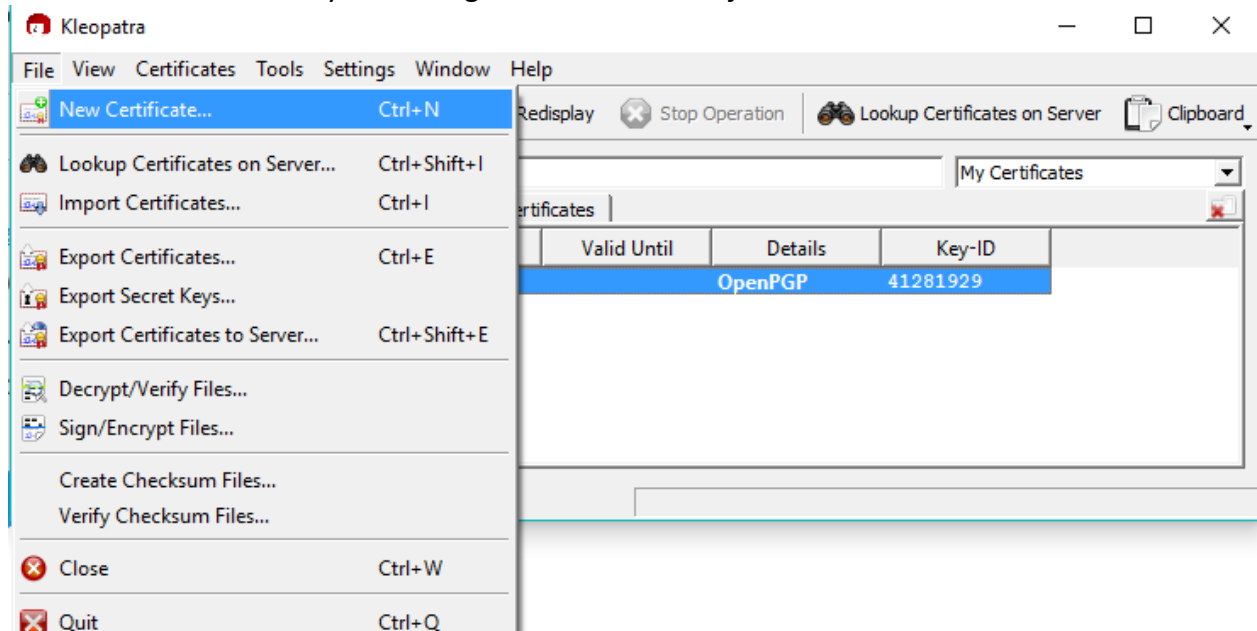
Berikut adalah panduan untuk melakukan enkripsi OpenPGP dengan menggunakan Windows (Kleopatra) dan juga Linux.

- **Membuat Key**

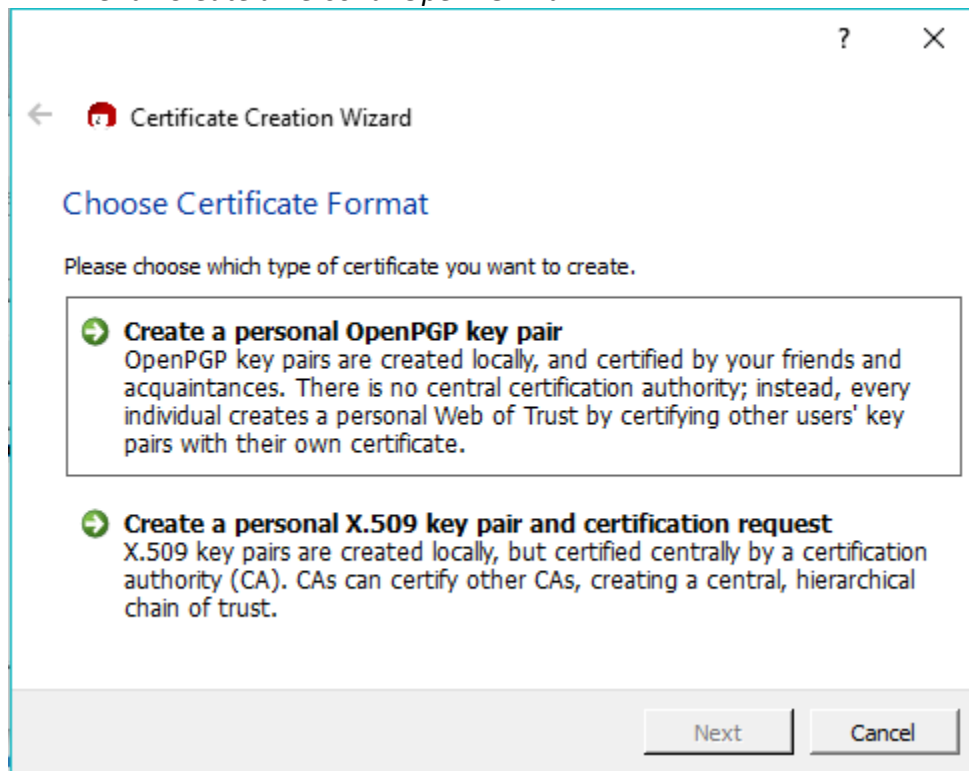
1. **Windows (Menggunakan Kleopatra)**

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

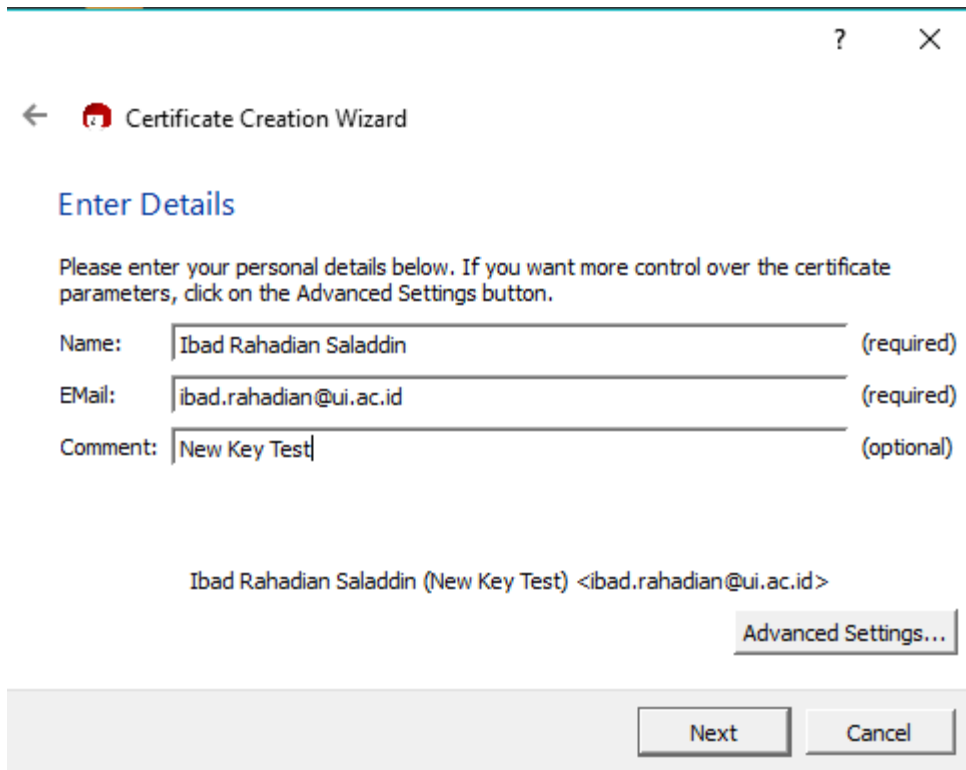
- a. Buka menu membuat key baru dengan *File -> New Certificate*.




- b. Pilih menu *"Create a Personal OpenPGP Pair"*



- c. Masukkan detail data diri Anda.



The screenshot shows the 'Enter Details' step of the Certificate Creation Wizard. It includes input fields for Name, Email, and Comment, with a summary line and an 'Advanced Settings...' button.

←  Certificate Creation Wizard

Enter Details

Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button.

Name: (required)

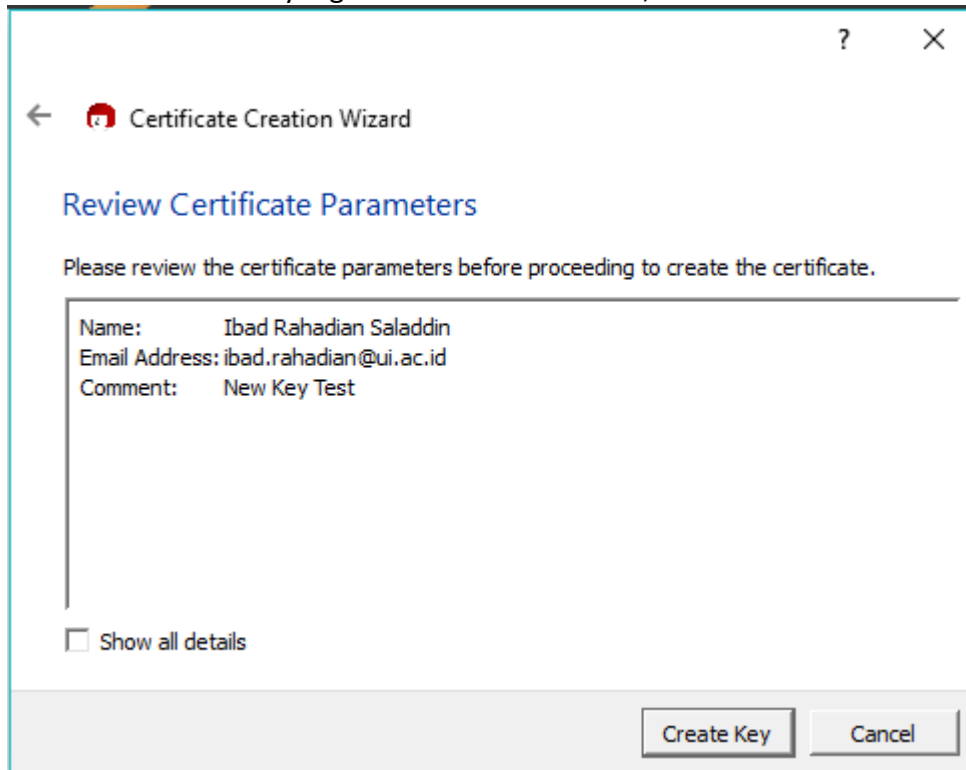
Email: (required)

Comment: (optional)


Ibad Rahadian Saladdin (New Key Test) <ibad.rahadian@ui.ac.id>

[Advanced Settings...](#)

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



The screenshot shows the 'Review Certificate Parameters' step of the Certificate Creation Wizard. It displays a summary of the entered details and a 'Show all details' checkbox.

←  Certificate Creation Wizard

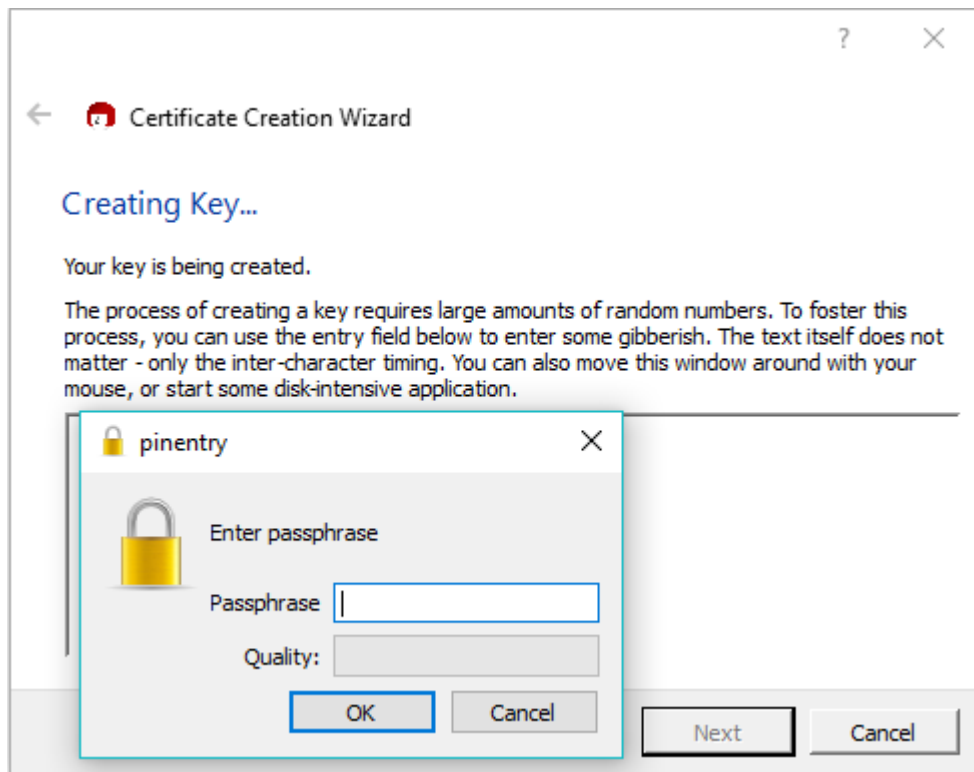
Review Certificate Parameters

Please review the certificate parameters before proceeding to create the certificate.

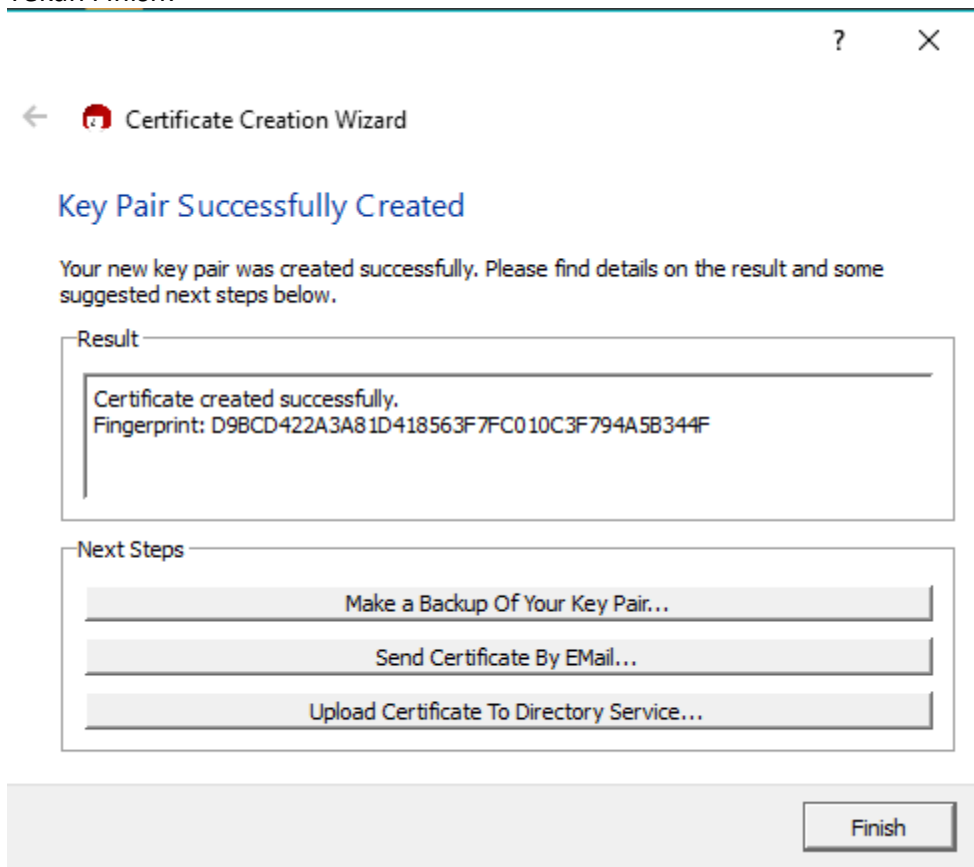
Name: Ibad Rahadian Saladdin
Email Address: ibad.rahadian@ui.ac.id
Comment: New Key Test

☐ Show all details

- e. Masukkan kata kunci Anda, jangan beritahukan kepada orang lain sebanyak dua kali.



f. Tekan *Finish*.

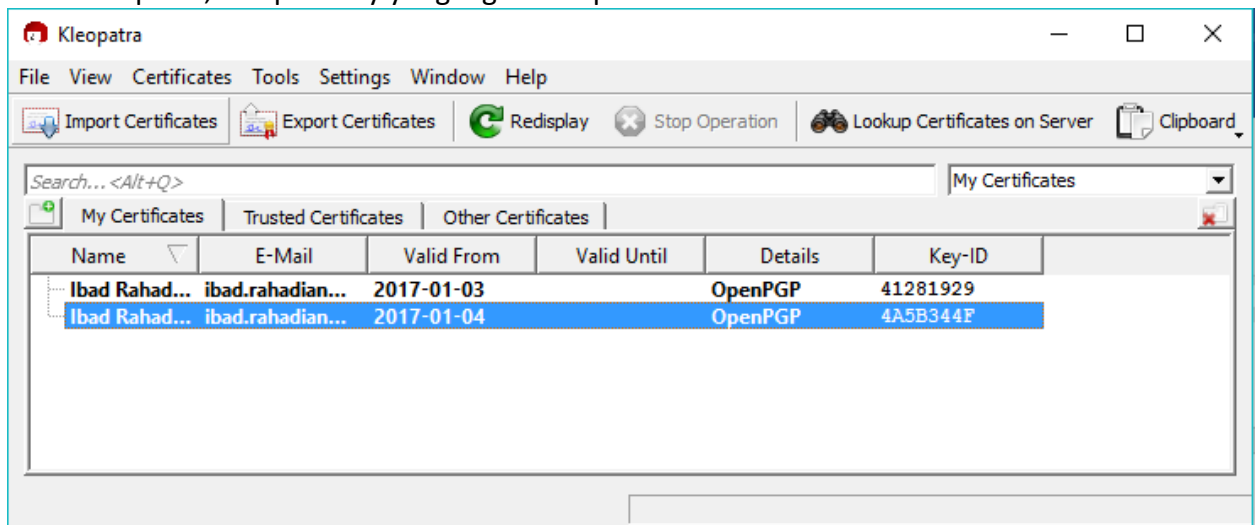


2. Linux

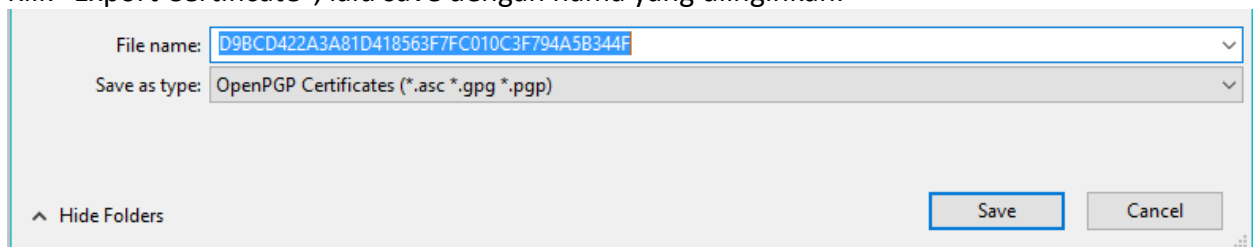
- **Export Key**

- 1. Windows (Menggunakan Kleopatra)**

- a. Buka Kleopatra, lalu pilih key yang ingin di-export.



- b. Klik "Export Certificate", lalu save dengan nama yang diinginkan.

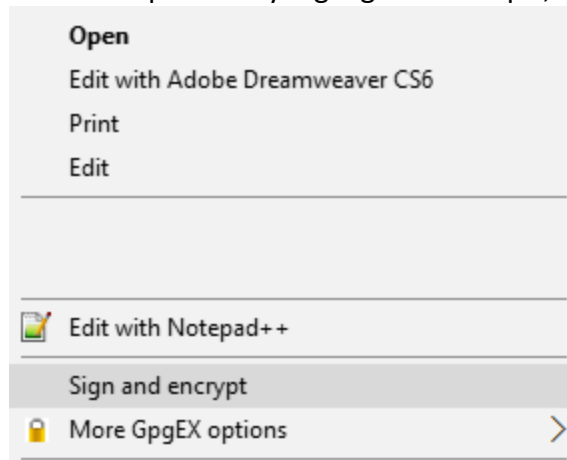


- 2. Linux**

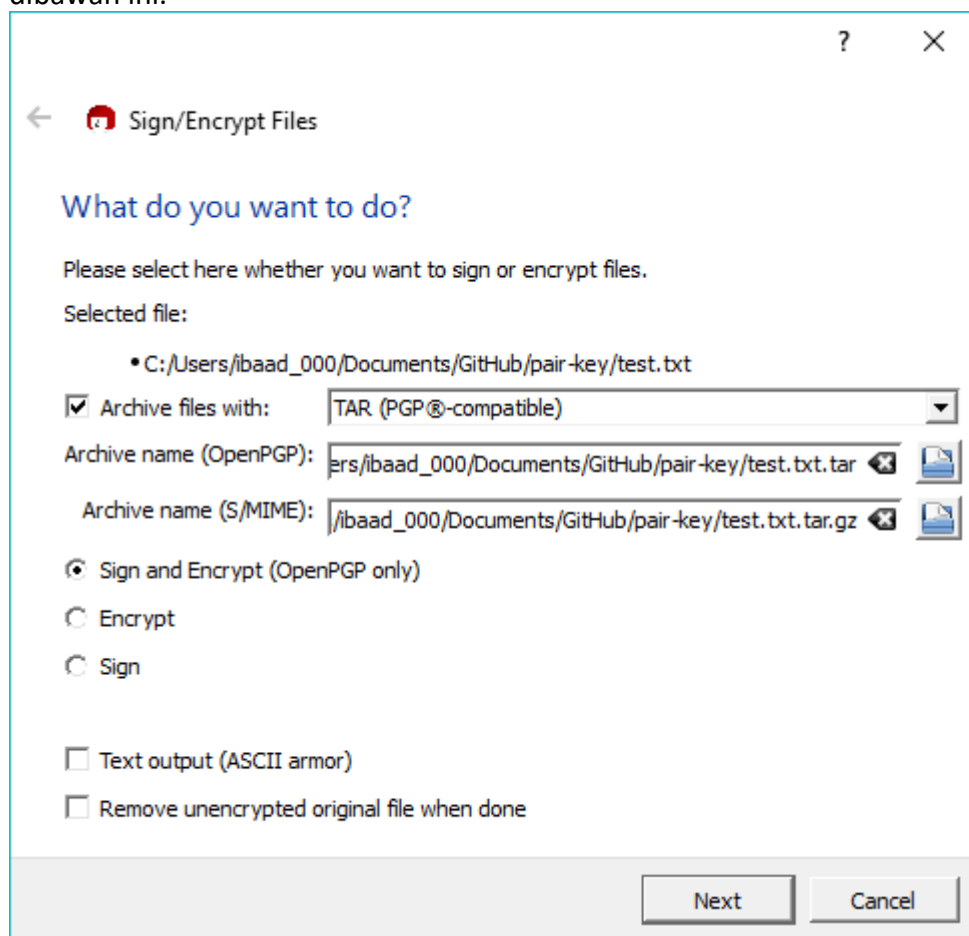
- Melakukan Enkripsi

1. Windows

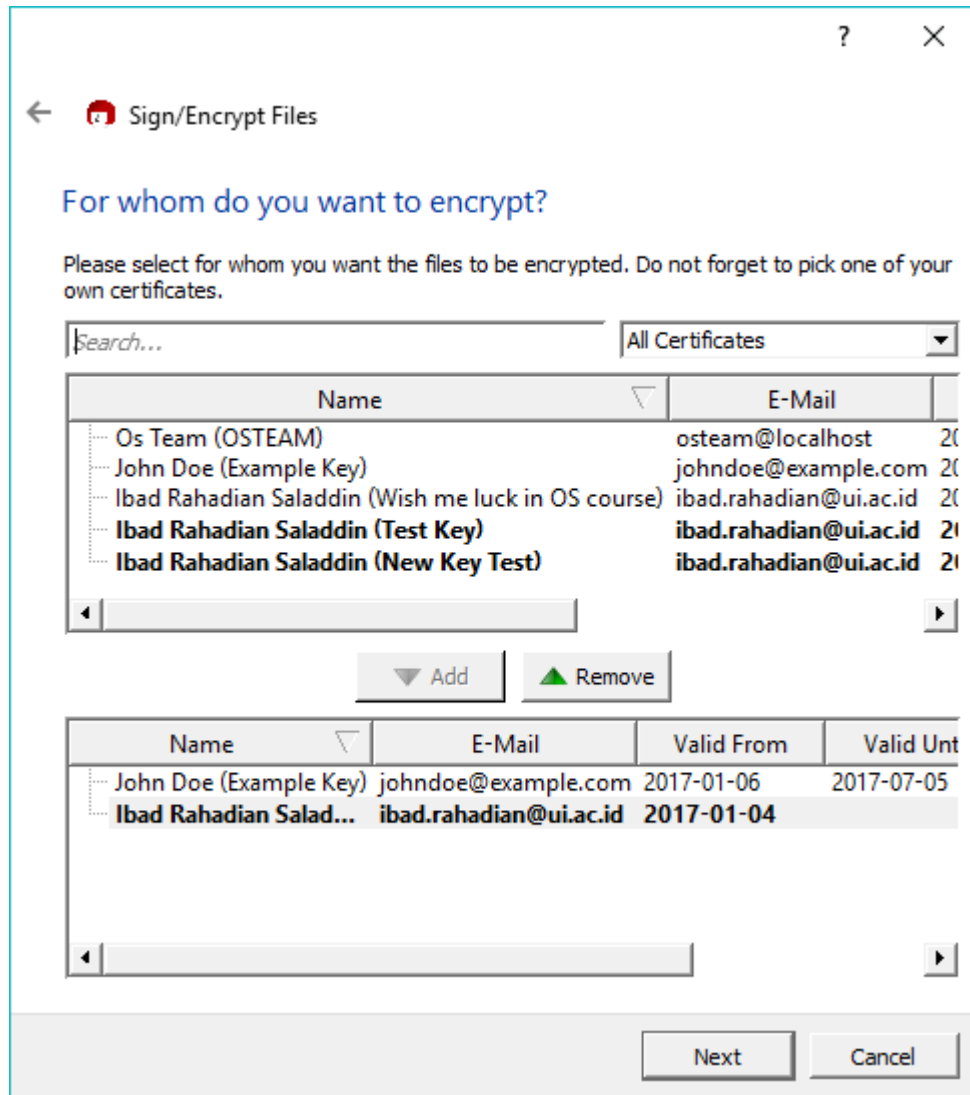
- a. Klik kanan pada file yang ingin di-enkripsi, lalu tekan *Sign and encrypt*



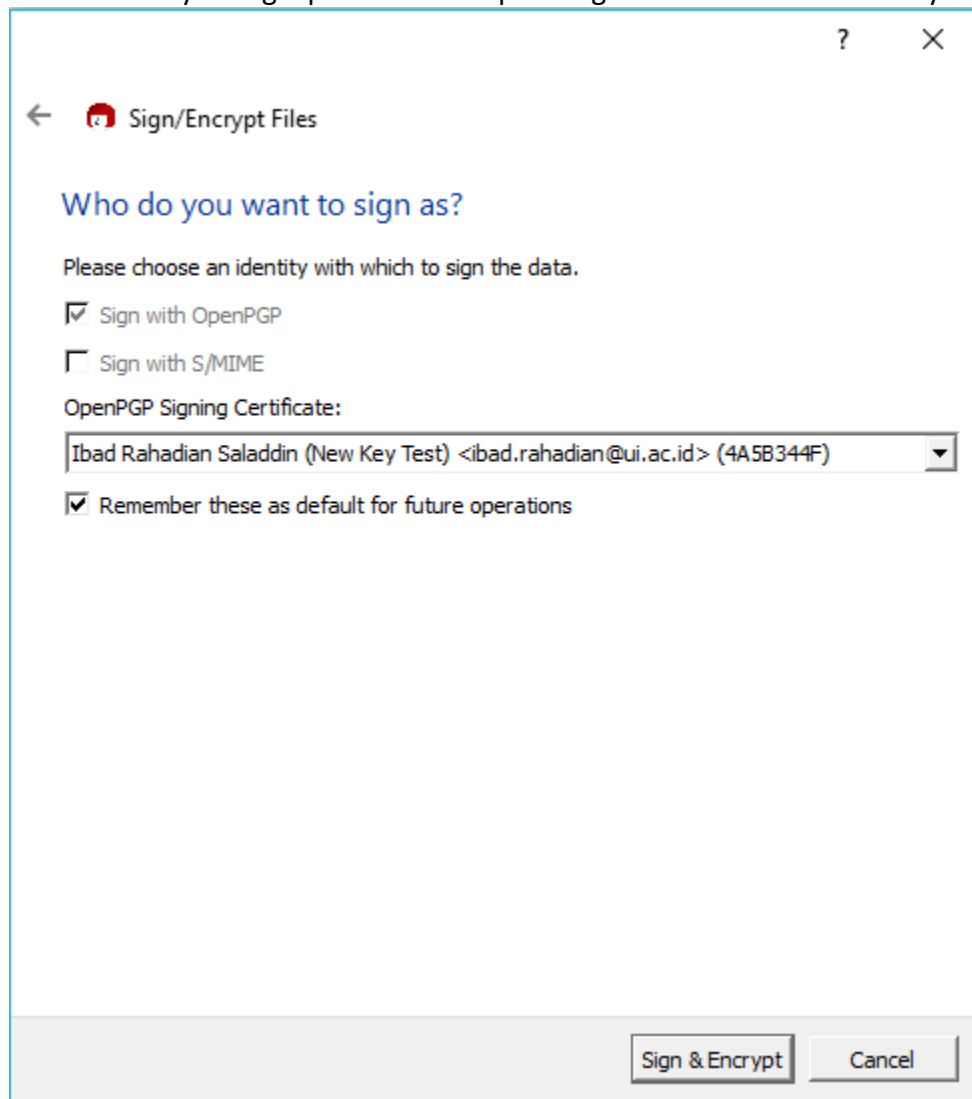
- b. Isi tujuan dan *Radio Button* "Sign and Encrypt (Open PGP only)" seperti pada gambar dibawah ini.



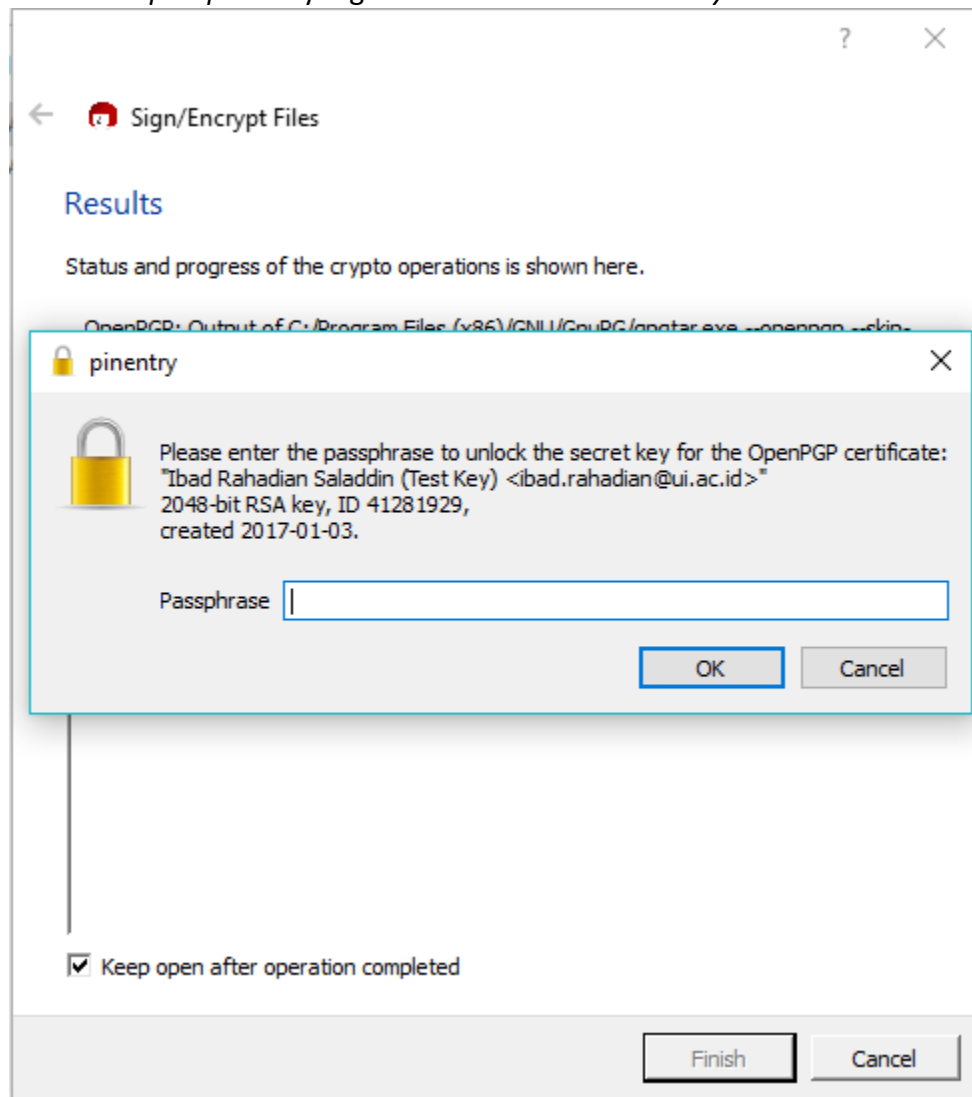
- c. Pilih *public key* user yang ingin dituju (termasuk diri sendiri) dengan me-klik tombol *Add*.



- d. Masukkan key sebagai pembuat enkripsi dengan memilih salah satu key.



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



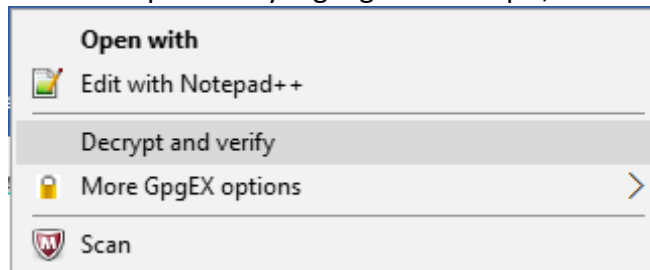
f. Silahkan tekan *Finish*. *File* telah ter-enkripsi.

2. Linux

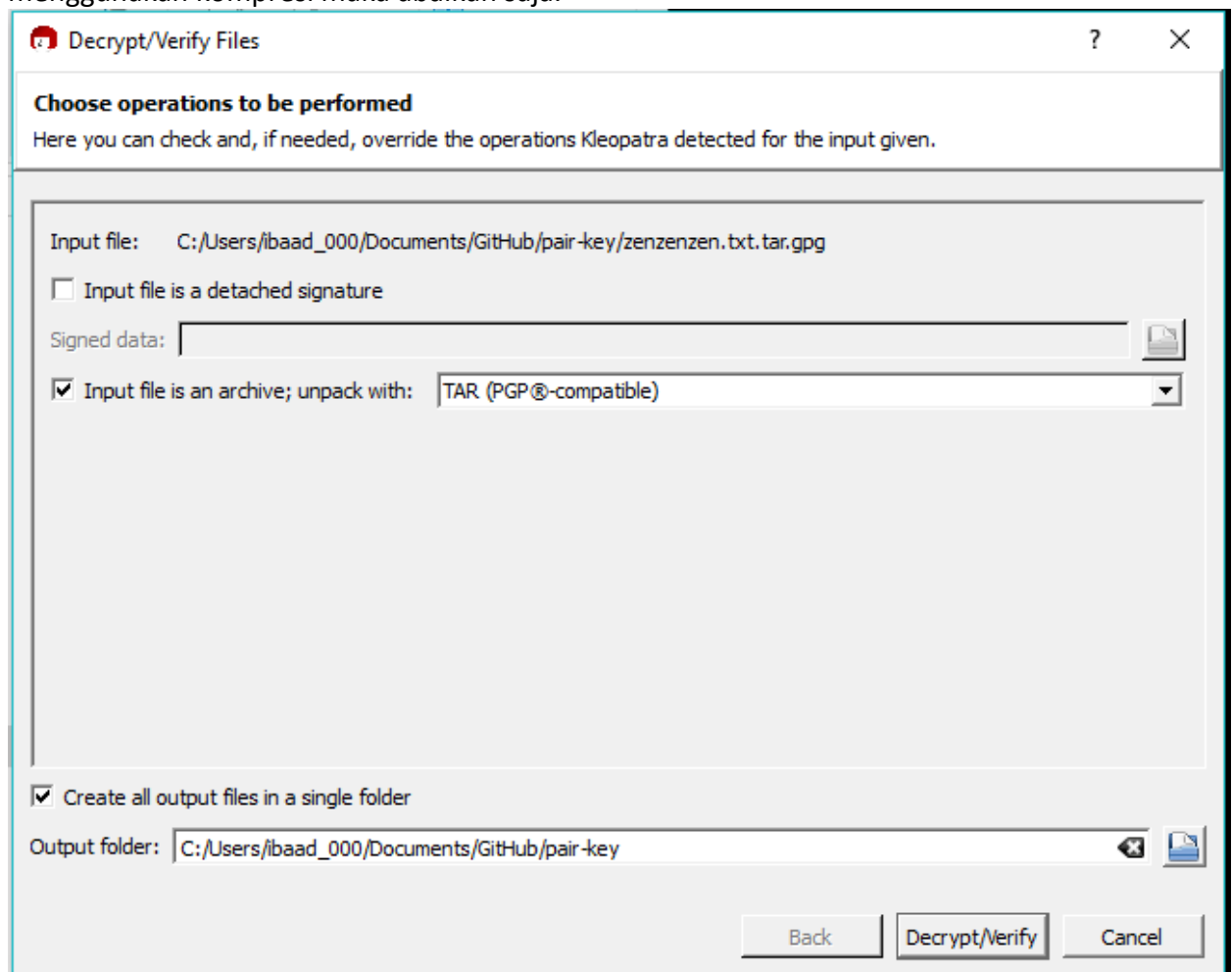
- **Melakukan Dekripsi**

- 1. Windows**

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



- b. 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.

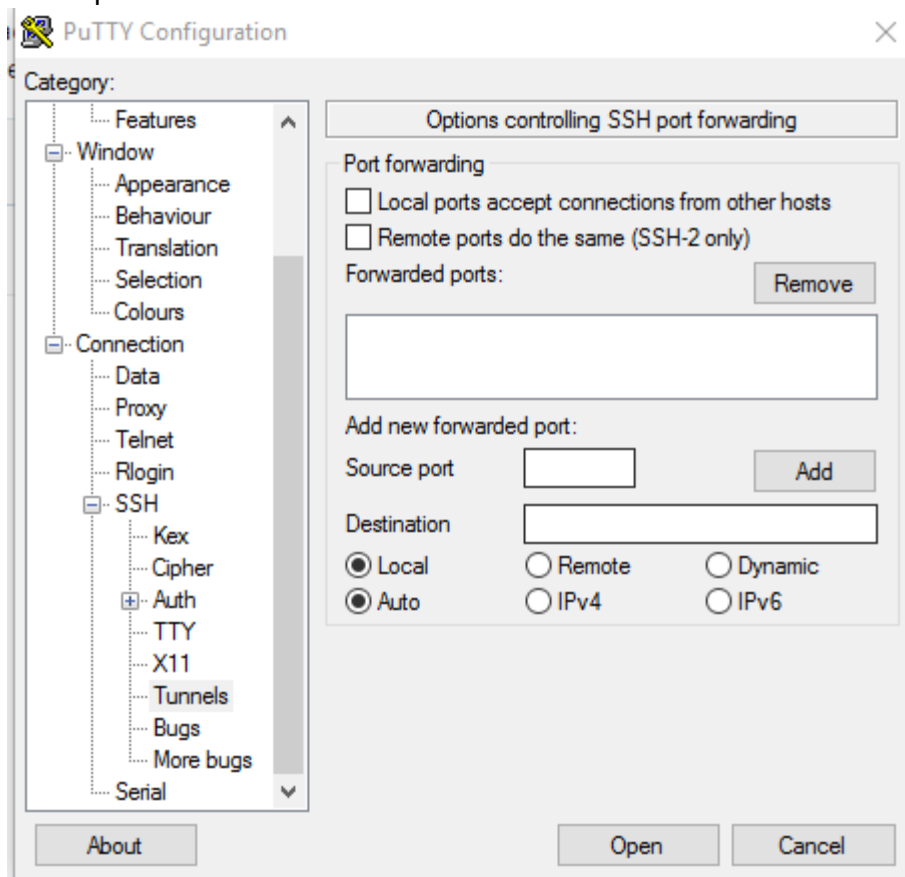


- c. Klik *Decrypt/Verify*.
- d. Masukkan *passphrase* yang dibuat pada awal pembuatan key.
- e. Klik *Finish*.

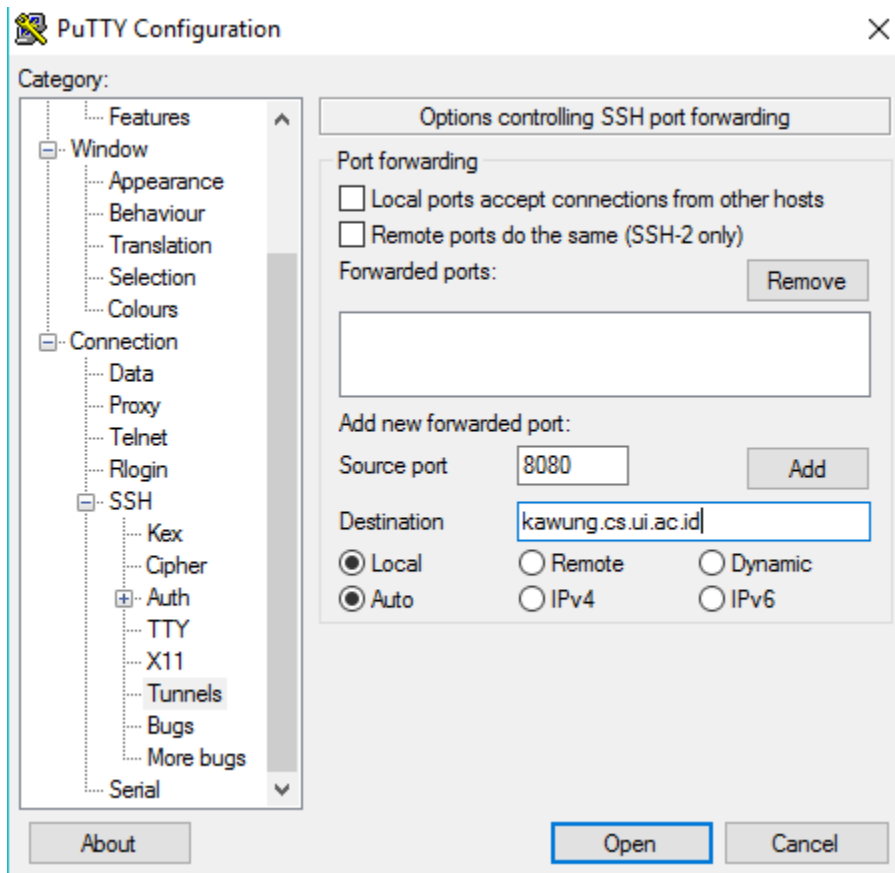
- 2. Linux**

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

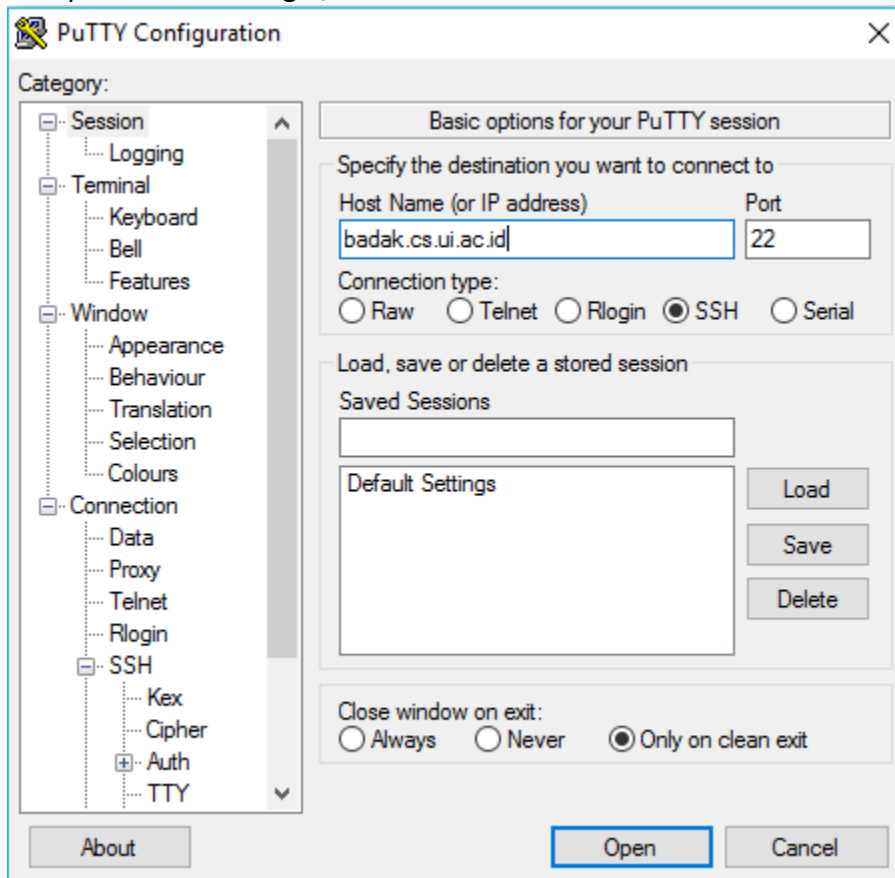
1. Buka aplikasi PuTTY



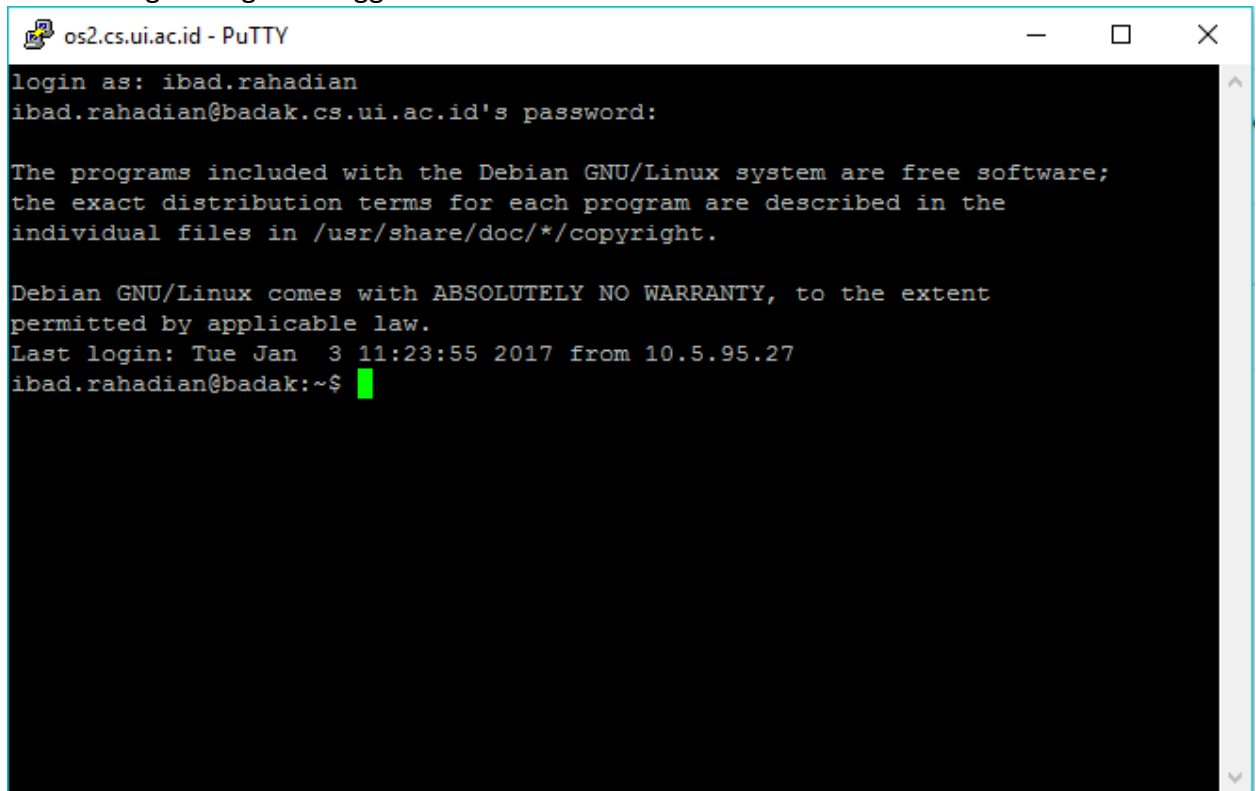
2. Pada kotak di sebelah kiri arahkan kepada halaman Connections -> SSH -> Tunnels, lalu masukkan port yang diinginkan dan nama server kawung.cs.ui.ac.id. Lalu, klik tombol *add*.



3. Lalu pada halaman login, lakukan akses ke halaman badak.cs.ui.ac.id, lalu klik *open*.



4. Lakukan login dengan menggunakan akun LDAP UI Anda.



The screenshot shows a PuTTY terminal window titled "os2.cs.ui.ac.id - PuTTY". The terminal output is as follows:

```
login as: ibad.rahadian
ibad.rahadian@badak.cs.ui.ac.id's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jan  3 11:23:55 2017 from 10.5.95.27
ibad.rahadian@badak:~$
```

The terminal shows a successful login for the user 'ibad.rahadian' from the IP address 10.5.95.27. The prompt is 'ibad.rahadian@badak:~\$'.