Nama Praktikan: Limas Baginta

NPM: 1306368690

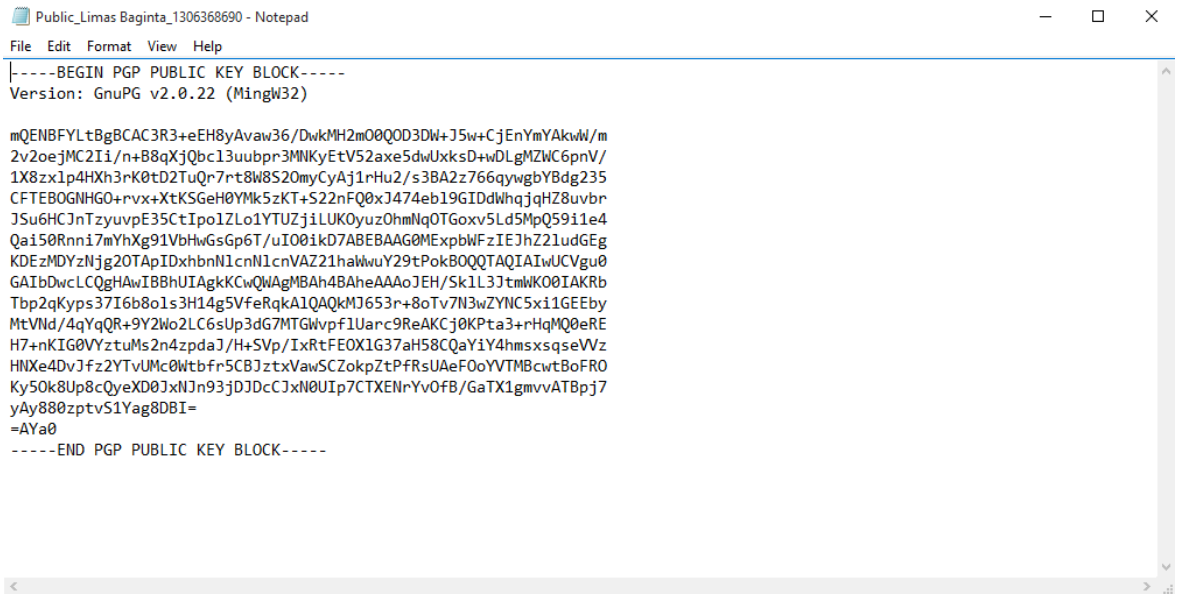
Praktikum: Keamanan Jaringan Komputer

Case Study danTugas Tambahan Modul 3

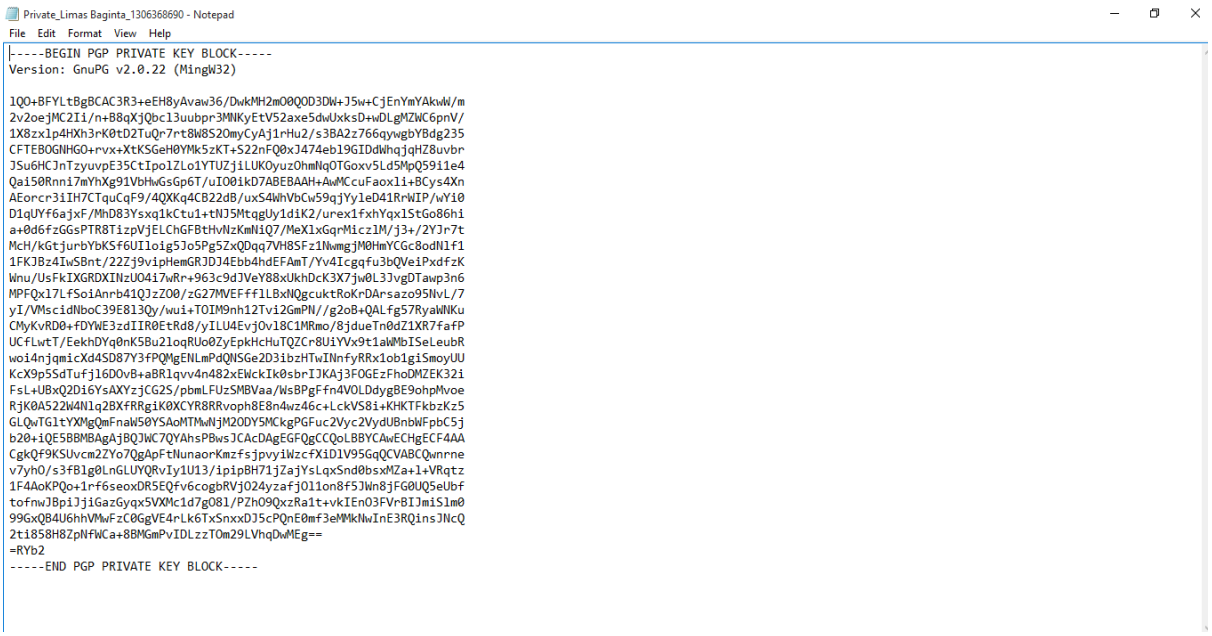
Percobaan (Case Study)

1 dan 2.

Public Key (**Diautentikasi Pandu Wicaksono)**

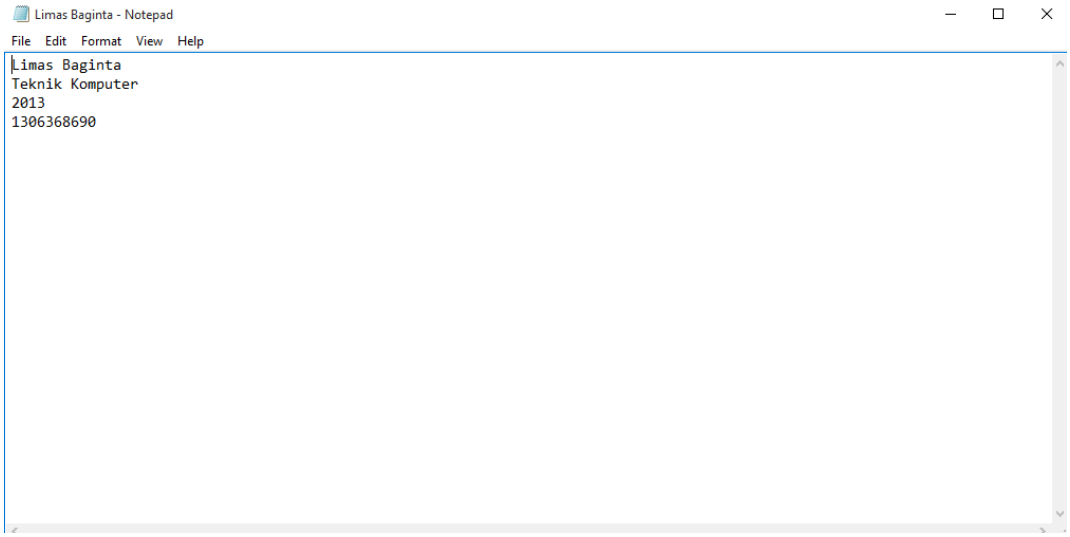


Private Key



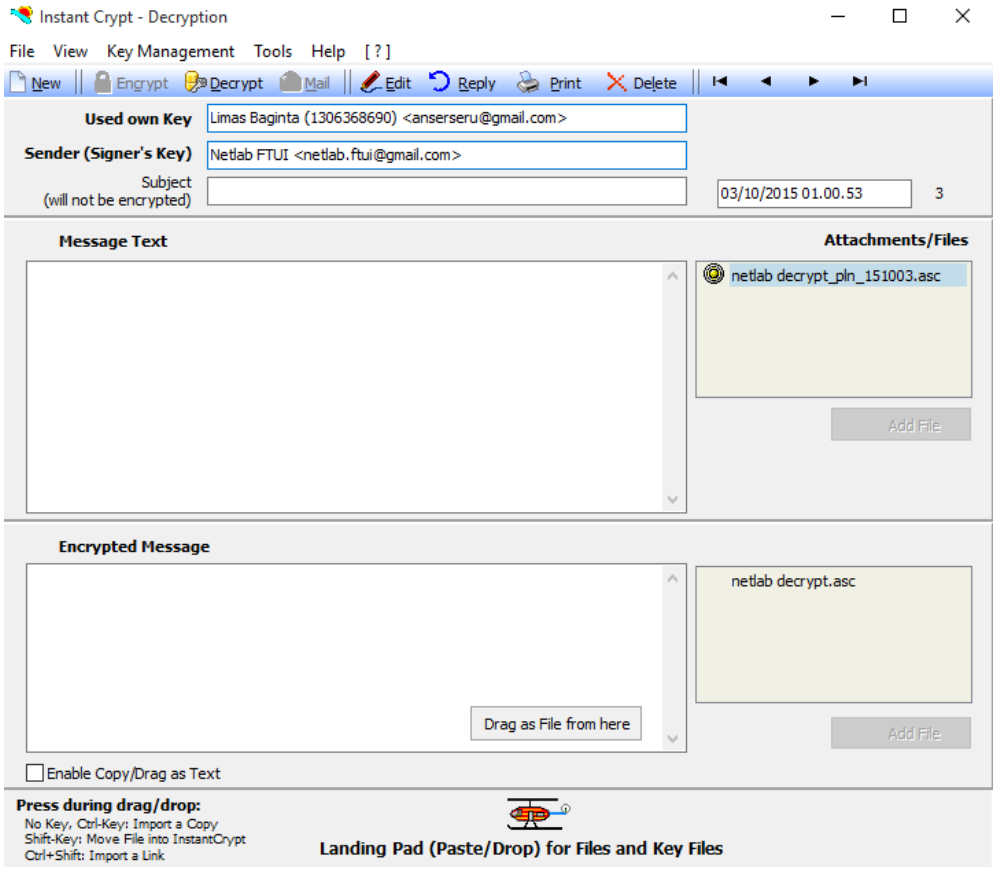
3 dan 4.

Isi pesan milik saya:

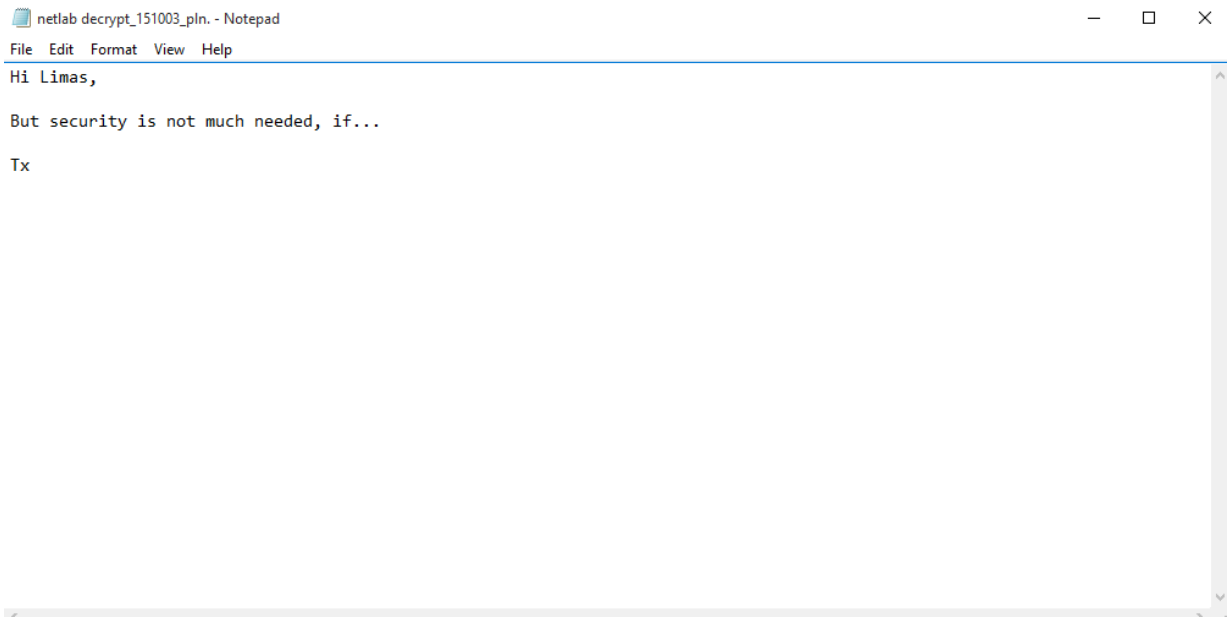


5.

Proses melakukan dekripsi Keyword Pesan yang didapat dari mentor dengan InstantCrypt



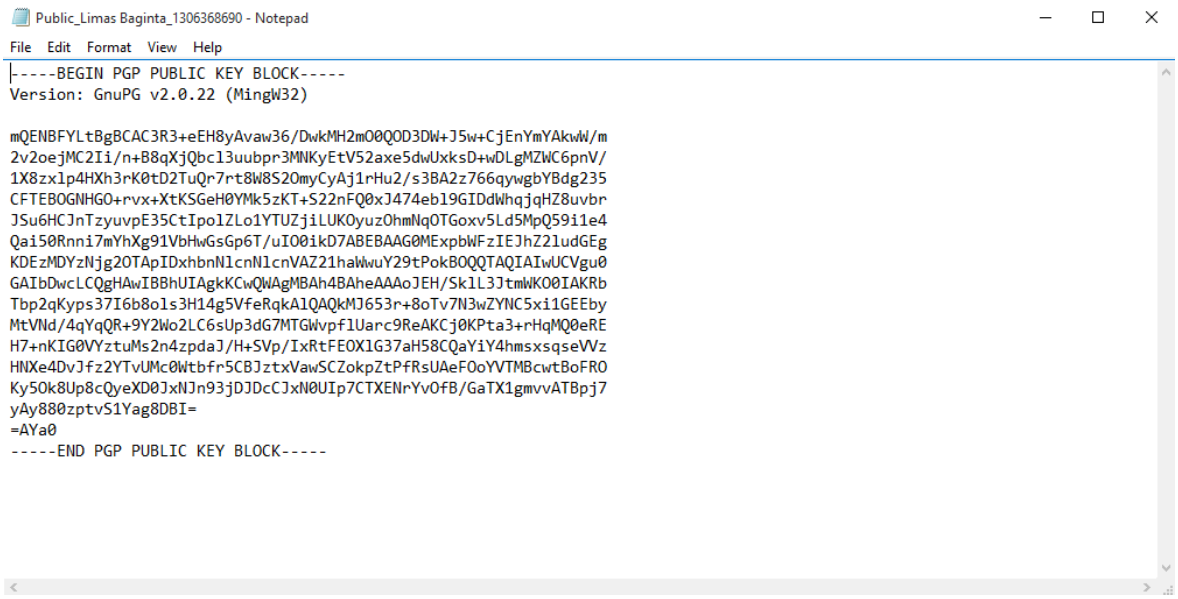
Isi pesan dari mentor sesudah di-dekripsi :



Tugas

1.Tampilkan screenshot isi Public dan Private Key anda ! (10)

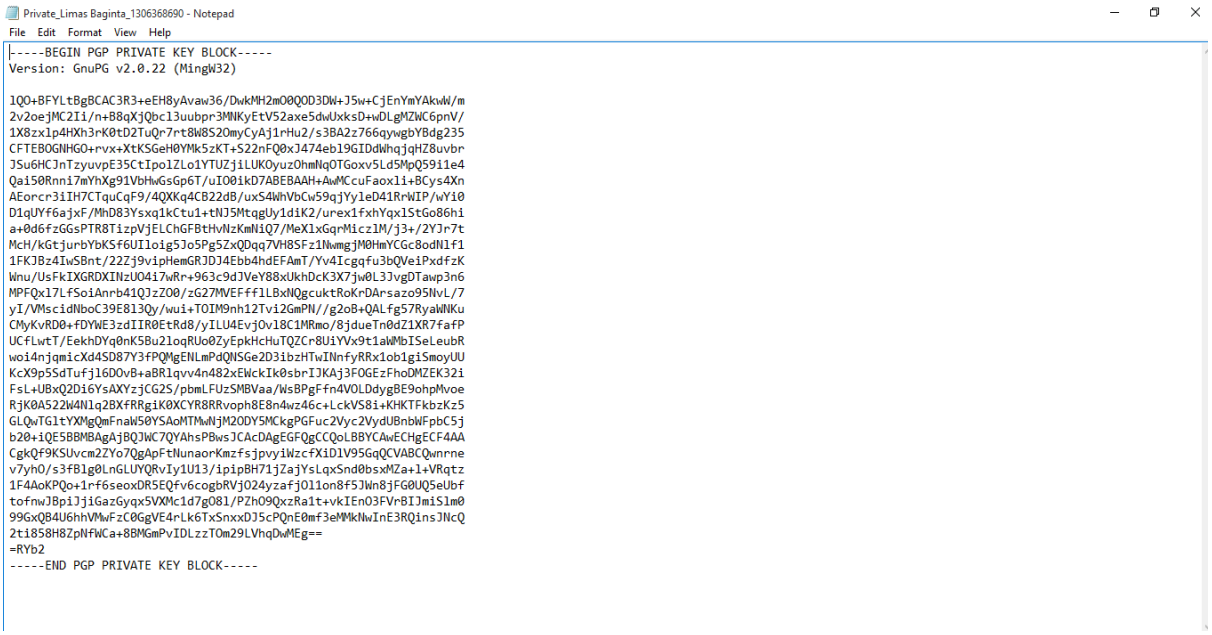
Public Key (**Diautentikasi Pandu Wicaksono)**


Public_Limas Baginta_1306368690 - Notepad

File Edit Format View Help

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (MingW32)

mQENBFYLtBgBCAC3R3+eEH8yAvaw36/DwkMH2mO0QOD3DW+J5w+CjEnYmYAkwW/m
2v2oejMC2Ii/n+B8qXjQbcl3uubpr3MNKyEtV52axe5dwUxksD+wDLgMZWC6pnV/
1X8zxlp4HXh3rK0tD2TuQr7rt8W8S2OmyCyAj1rHu2/s3BA2z766qywgbYBdg235
CFTEBOGNHGO+rvx+XtKSGeH0YMk5zKT+S22nFQ0xJ474eb19GIDdWhqjqHZ8uvbr
JSu6HCJnTzyuvpE35CtIpolZLo1YTUZjiLUKOyuzOhmNqOTGoxv5Ld5MpQ59i1e4
Qai50Rnni7mYhXg91VbHwGsGp6T/uIO0ikD7ABEBAAG0MExpbWFzIEJhZ2ludGEg
KDEzMDYzNjg2OTApIDxhbnNlcnNlcnVAZ21haWwuY29tPokBOQQTAQIAIwUCVgu0
GAIbDwcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheAAAoJEH/Sk1L3JtmWKO0IAKRb
Tbp2qKyps37I6b8ols3H14g5VfeRqkAlQAQkMJ653r+8oTv7N3wZYNC5xi1GEEby
MtVNd/4qYqQR+9Y2Wo2LC6sUp3dG7MTGWvpflUarc9ReAKCj0KPta3+rHqMQ0eRE
H7+nKIG0VYztuMs2n4zpdaJ/H+SVp/IxRtFEOXlG37aH58CQaYiY4hmsxsqseVVz
HNXe4DvJfz2YTvUMc0Wtbfr5CBJztxVawSCZokpZtPfRsUAeFOoYVTMBcwtBoFRO
Ky5Ok8Up8cQyeXD0JxNJn93jDJDcCJxN0UIp7CTXENrYvOfB/GaTX1gmvvATBpj7
yAy880zptvS1Yag8DBI=
=AYa0
-----END PGP PUBLIC KEY BLOCK-----
```

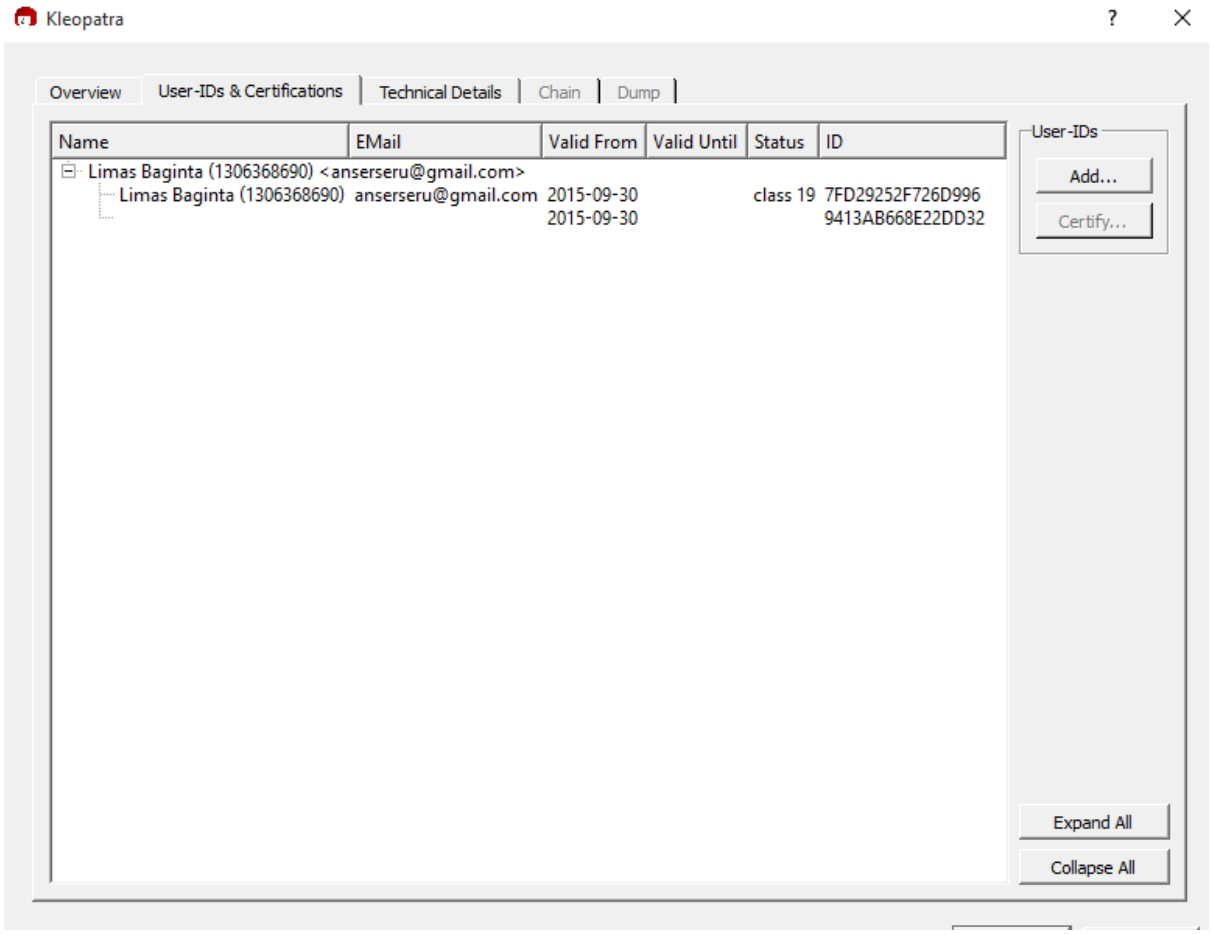
Private Key


Private_Limas Baginta_1306368690 - Notepad

File Edit Format View Help

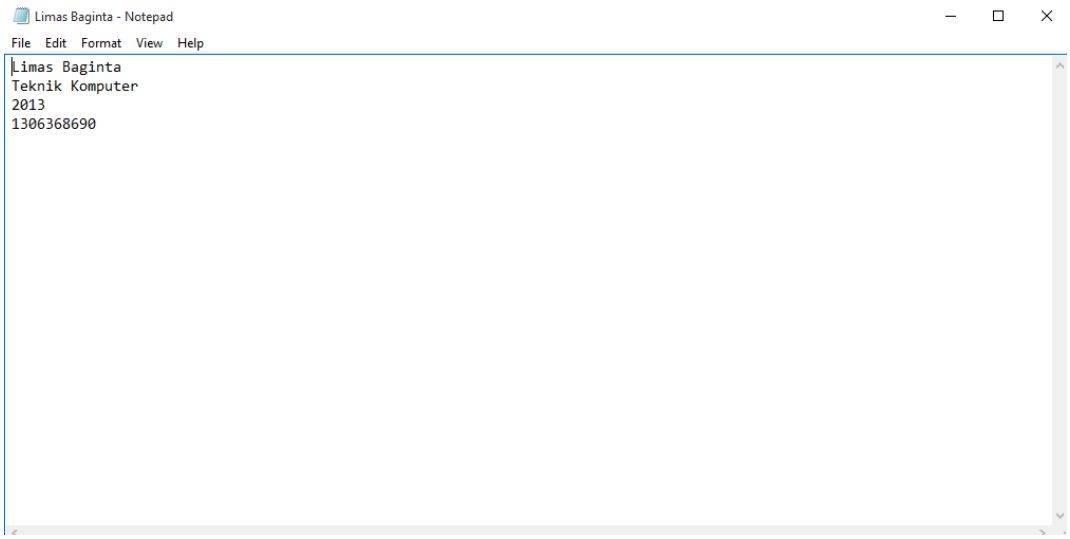
```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: GnuPG v2.0.22 (MingW32)

lQO+BFYLtBgBCAC3R3+eEH8yAvaw36/DwkMH2mO0QOD3DW+J5w+CjEnYmYAkwW/m
2v2oejMC2Ii/n+B8qXjQbcl3uubpr3MNKyEtV52axe5dwUxksD+wDLgMZWC6pnV/
1X8zxlp4HXh3rK0tD2TuQr7rt8W8S2OmyCyAj1rHu2/s3BA2z766qywgbYBdg235
CFTEBOGNHGO+rvx+XtKSGeH0YMk5zKT+S22nFQ0xJ474eb19GIDdWhqjqHZ8uvbr
JSu6HCJnTzyuvpE35CtIpolZLo1YTUZjiLUKOyuzOhmNqOTGoxv5Ld5MpQ59i1e4
Qai50Rnni7mYhXg91VbHwGsGp6T/uIO0ikD7ABEBAAH+AwMCcuFaoxli+BCys4Xn
AEorcr3iIH7CTquCqF9/4QXKq4CB22dB/uxS4WhVbCw59qjYyleD41RrWIP/wYi0
D1qUYf6ajxF/MhD83Ysxq1kCtu1+tNJ5MtqgUy1diK2/urex1fxhYqxlStGo86hi
a+0d6fzGGsPTR8TizpVjELChGFBtHvNzKmNiQ7/MeX1xGqrMicz1M/j3+/2YJr7t
McH/kGtjurbYbKSf6UIloig5Jo5Pg5ZxQDqq7VH8SFz1NwmgjM0HmYCGc8odN1f1
1FKJBz4IwSBnt/22Zj9vipHemGRJDJ4Ebb4hdEFAmT/Yv4Icgqfu3bQVeiPxdfzK
Wnu/UsFkIXGRDXINzUO4i7wRr+963c9dJVeY88xUkhDcK3X7jw0L3JvgDTawp3n6
MPFQxl7LfSoiAnrb41QJzZO0/zG27MVEFffLLBxNQgcuktRoKrDArsazo95NvL/7
yI/VMscidNboC39E8l3Qy/wui+TOIM9nh12Tvi2GmPN//g2oB+QALfg57RyaWNKu
CMyKvRD0+fDYWE3zdIIR0EtRd8/yILU4EvjOvl8C1MRmo/8jdueTn0dZ1XR7fafP
UCfLwtT/EekhDYq0nK5Bu2loqRUo0ZyEpkHcHuTQZCr8UiYVx9t1aWMbISeLeubR
woi4njqmicXd4SD87Y3fPQMgENLmPdQNSGe2D3ibzHTwINnfyRRx1ob1giSmoyUU
KcX9p5SdTufjl6DOvB+aBR1qvv4n482xEWckIk0sbrIJKAj3FOGEzFhoDMZEK32i
FsL+UBxQ2Di6YsAXYzjCG2S/pbmLFUzSMBVaa/WsBPgFfn4VOLDdygBE9ohpMvoe
RjK0A522W4Nlq2BXfRRgiK0XCYR8RRvoph8E8n4wz46c+LckVS8i+KHKTFkbzKz5
GLQwTGltYXMgQmFnaW50YSAoMTMwNjM2ODY5MCkgPGFuc2Vyc2VydUBnbWFpbC5j
b20+iQE5BBMBAgAjBQJWC7QYAhsPBwsJCAcDAgEGFQgCCQoLBBYCAwECHgECF4AA
CgkQf9KSUvcm2ZYo7QgApFtNunaorKmzfsjpvyiWzcfXiDlV95GqQCVABCQwnrne
v7yhO/s3fBlg0LnGLUYQRvIy1U13/ipipBH71jZajYsLqxSnd0bsxMZa+l+VRqtz
1F4AoKPQo+1rf6seoxDR5EQfv6cogbRVjO24yzafjO11on8f5JWn8jFG0UQ5eUbf
tofnwJBpiJjiGazGyqx5VXMc1d7gO8l/PZhO9QxzRa1t+vkIEnO3FVrBIJmiS1m0
99GxQB4U6hhVMwFzC0GgVE4rLk6TxSnxxDJ5cPQnE0mf3eMMkNwInE3RQinsJNcQ
2ti858H8ZpNfWCa+8BMGmPvIDLzzTOm29LVhqDwMEg==
=RYb2
-----END PGP PRIVATE KEY BLOCK-----
```

2. Tampilkan screenshot bukti bahwa Public Key anda telah terautentikasi ! (10)

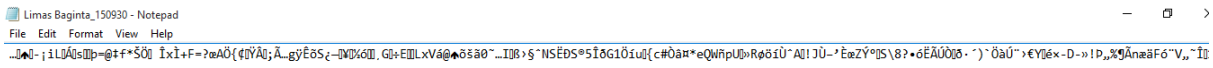


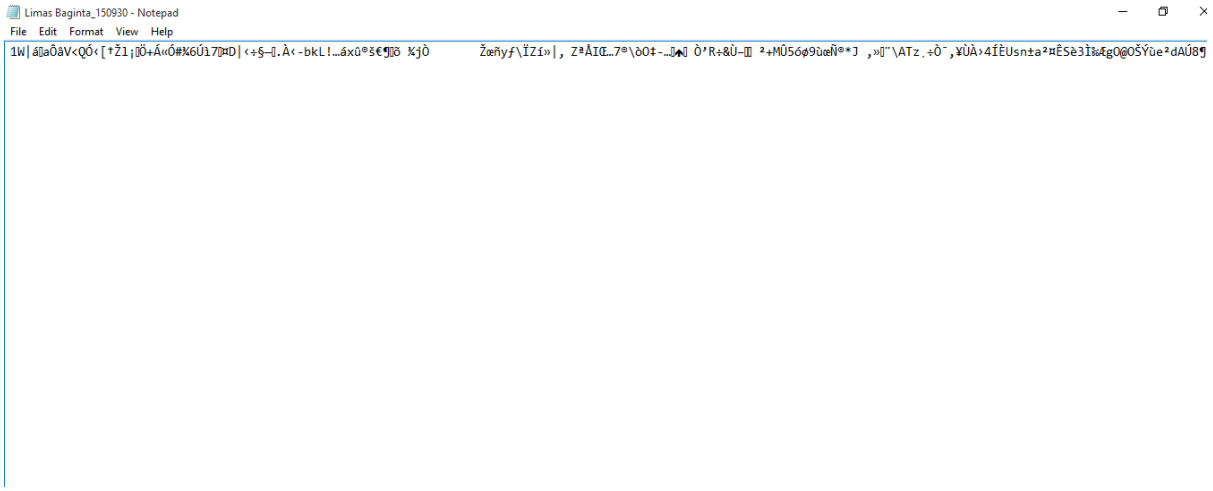
3. Tuliskan isi pesan anda sebelum dan sesudah di-enkripsi ! (20)

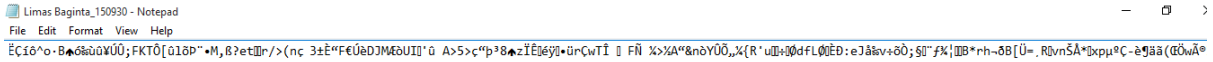
Isi pesan sebelum di-enkripsi :



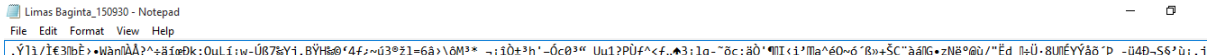
Isi pesan sesudah di-enkripsi :

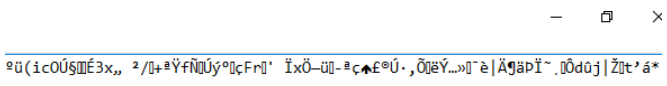





Limas Baginta_150930 - Notepad
File Edit Format View Help

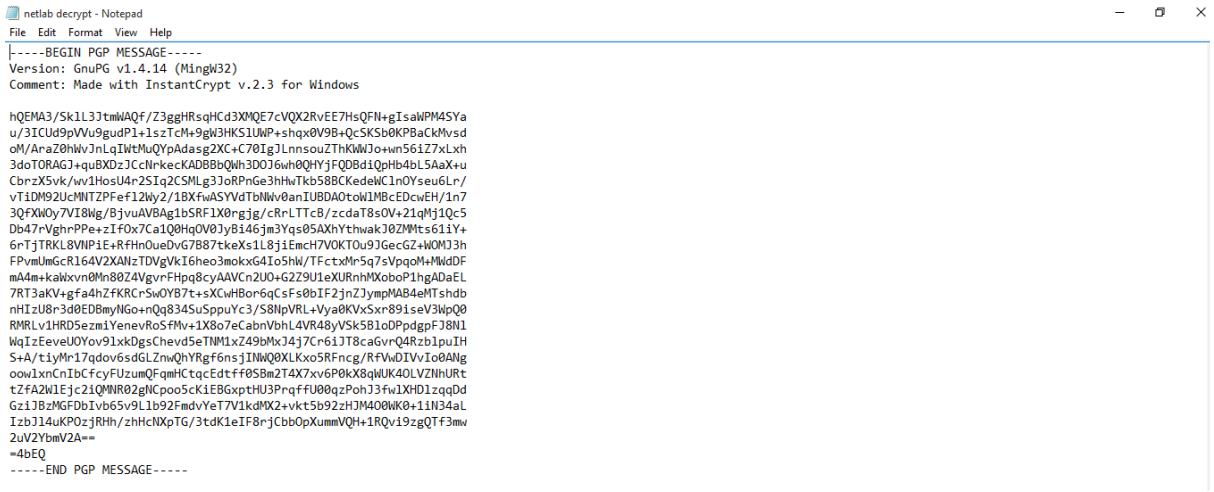

Limas Baginta_150930 - Notepad
ile Edit Format View Help


Limas Baginta_150930 - Notepad
File Edit Format View Help



4. Tuliskan isi pesan (keyword) dari mentor sebelum dan sesudah di-dekripsi ! Apa bukti bahwa pesan tersebut belum dimodifikasi oleh siapa pun? (30)

Isi pesan (keyword)dari mentor sebelum di-dekripsi :



-----BEGIN PGP MESSAGE-----

Version: GnuPG v1.4.14 (MingW32)

Comment: Made with InstantCrypt v.2.3 for Windows

hQEMA3/SklL3JtmWAQf/Z3ggHRsqHCd3XMQE7cVQX2RvEE7HsQFN+gIsaWPM4SYa

u/3ICUd9pVVu9gudPl+lszTcM+9gW3HKSlUWP+shqx0V9B+QcSKSb0KPBaCkMvsd

oM/AraZ0hWvJnLqIWtMuQYpAdasg2XC+C70lgJLnnsouZThKWWJo+wn56iZ7xLxh

3doTORAGJ+quBXDzJCcNrkecKADBBbQWh3DOJ6wh0QHYjFQDBdiQpHb4bL5AaX+u

CbrzX5vk/wv1HosU4r2SIq2CSMLg3JoRPnGe3hHwTkb58BCKedeWClnOYseu6Lr/

vTiDM92UcMNTZPFefl2Wy2/1BXfwASYVdTbNWv0anIUBDAOtoWlMBcEDcwEH/1n7

3QfXWOy7VI8Wg/BjvuAVBAg1bSRFlX0rgjg/cRrLTTcB/zcdaT8sOV+21qMj1Qc5

Db47rVghrPPe+zIfOx7Ca1Q0HqOV0JyBi46jm3Yqs05AXhYthwakJ0ZMMts61iY+

6rTjTRKL8VNPiE+RfHnOueDvG7B87tkeXs1L8jiEmcH7VOKTOu9JGecGZ+WOMJ3h

FPvmUmGcRl64V2XANzTDVgVkI6heo3mokxG4Io5hW/TFctxMr5q7sVpqoM+MWdDF

mA4m+kaWxvn0Mn80Z4VgvrFHpq8cyAAVCn2UO+G2Z9U1eXURnhMXoboP1hgADaEL

7RT3aKV+gfa4hZfKRCrSwOYB7t+sXCwHBor6qCsFs0bIF2jnZJympMAB4eMTshdb

nHIzU8r3d0EDBmyNGo+nQq834SuSppuYc3/S8NpVRL+Vya0KVxSxr89iseV3WpQ0

RMRLv1HRD5ezmiYenevRoSfMv+1X8o7eCabnVbhL4VR48yVSk5BloDPpdgpFJ8Nl

WqIzEeveUOYov9lxkDgsChevd5eTNM1xZ49bMxJ4j7Cr6iJT8caGvrQ4RzblpuIH

S+A/tiyMr17qdov6sdGLZnwQhYRgf6nsjINWQ0XLKxo5RFncg/RfVwDIVvIo0ANg

oowlxnCnIbCfcyFUzumQFqmHCtqcEdtff0SBm2T4X7xv6P0kX8qWUK4OLVZNhURt

tZfA2WlEjc2iQMNR02gNCpoo5cKiEBGxptHU3PrqffU00qzPohJ3fwlXHDlzqqDd

GziJBzMGFDbIvb65v9Llb92FmdvYeT7V1kdMX2+vkt5b92zHJM4O0WK0+1iN34aL

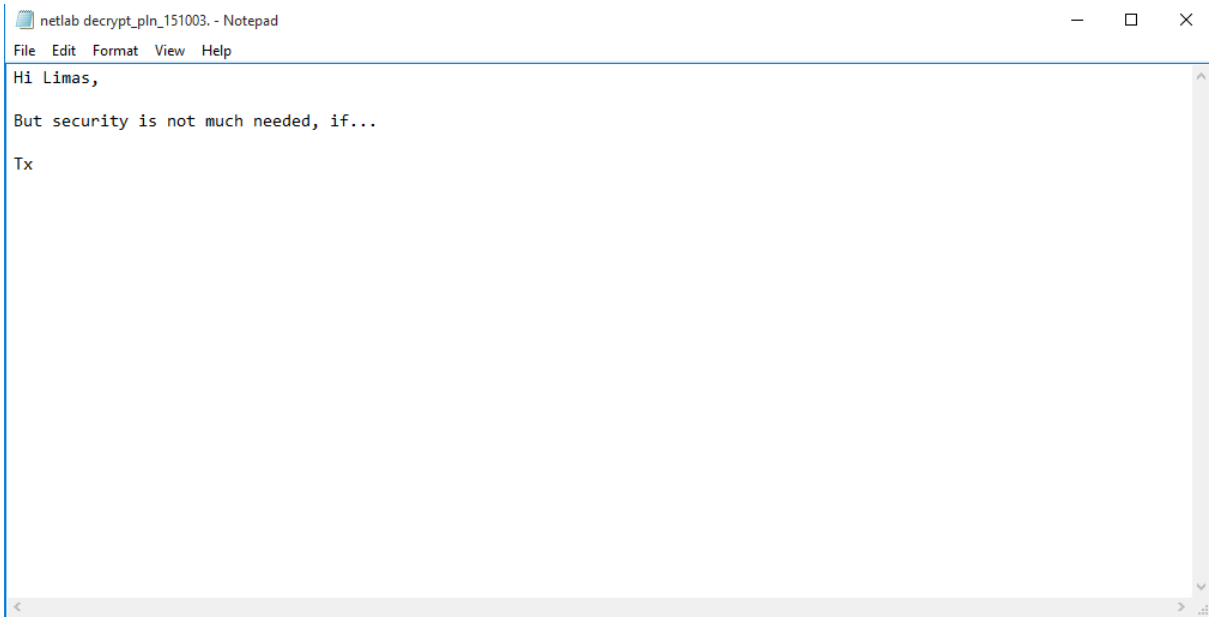
IzbJl4uKPOzjRHh/zhHcNXpTG/3tdK1eIF8rjCbbOpXummVQH+1RQvi9zgQTf3mw

2uV2YbmV2A==

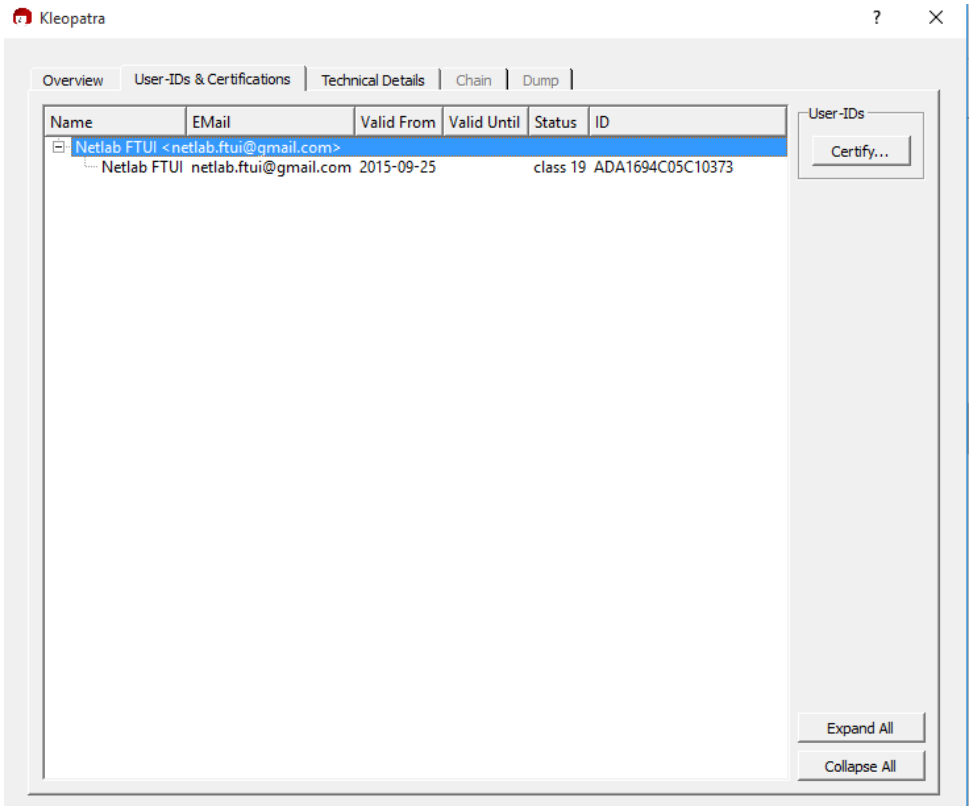
=4bEQ

-----END PGP MESSAGE-----

Isi pesan (keyword)dari mentor sesudah di-dekripsi :



Bukti bahwa pesan tersebut belum dimodifikasi oleh siapa pun:



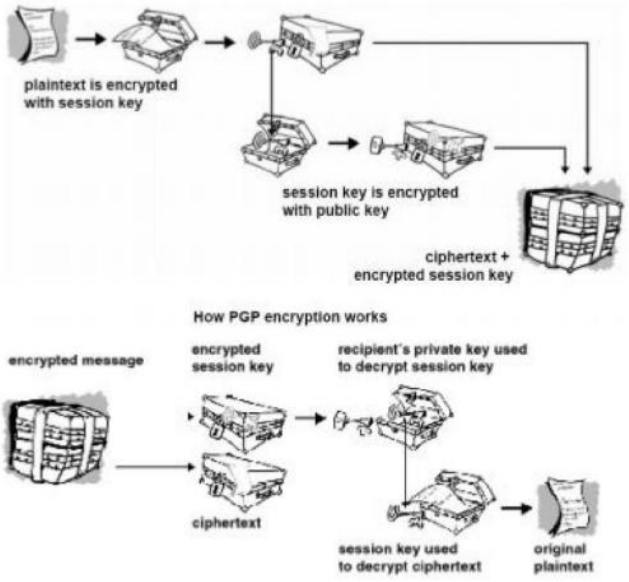
Untuk melihat bahwa pesan tersebut belum dimodifikasi oleh siapa pun adalah dengan cara mengecek autentikasi public key milik Netlab FTUI dan melihat Nama yang sudah melakukan sertifikasi public key tersebut.

Pada gambar terlihat bahwa pesan hanya disertifikasi Netlab FTUI tanpa adanya sertifikasi dari akun lain.
Jika pesan yang belum didekripsi cocok dengan public key milik Netlab FTUI maka dapat dipastikan bahwa pesan tersebut belum dimodifikasi oleh siapa pun

5. Jelaskan prosedur Sign – Encrypt – Decrypt – Verify pesan menggunakan PGP ! (30)

PGP (Pretty Good Privacy) adalah suatu metode enkripsi yang menyimpan kerahasiaan suatu informasi agar tidak dapat diketahui/dibaca oleh pihak selain pengirim dan penerima informasi. Informasi ini bisa berupa Email rahasia, nomor kode kartu kredit, atau pengiriman dokumen rahasia perusahaan melalui internet.

PGP menggunakan metode asymmetric cryptography, yang memiliki sistem pasangan public key dan private key. Setiap orang yang akan berkomunikasi menggunakan metode PGP harus memiliki sepasang kunci ini. Public key merupakan kunci yang dipublikasikan dan digunakan oleh orang lain untuk melakukan enkripsi pesan yang ditujukan kepada pemilik public key tersebut. Untuk men-dekripsi pesan tersebut, si penerima harus menggunakan private key milik-nya yang tidak boleh diketahui oleh orang lain. Berbeda dengan metode symmetric cryptography dimana proses enkripsi dan dekripsi hanya melibatkan satu buah kunci, sehingga si pengirim dan penerima harus bertukar kunci terlebih dahulu yang sangat beresiko karena dapat di-intercept oleh pihak lain di dalam jaringan.



Proses Encryption – Decryption pada PGP/GnuPG

Melakukan Sign

1. Buka Kleopatra
2. Klik File > New Certificate..
3. Di kotak dialog, pilih opsi Create a Personal OpenPGP key pair
4. Masukkan detail key
5. Klik Next > Create Key, masukkan passphrase. Harus menyertakan karakter angka.
6. Akan muncul kotak dialog, pilih Make a Backup Of Your Key Pair untuk meng-export key
7. Masukkan direktori. Centang opsi ASCII armor untuk tipe file *.asc ; kosongkan untuk tipe file *.pgp atau *.gpg.
8. Private key sudah dibuat. Untuk mengexport Public key, klik kanan pada certificate dan pilih Export Certificate.

Melakukan Enkripsi & Dekripsi Pesan

1. Buka InstantCrypt
2. Klik Key Management > Import Key untuk memasukkan key
3. Enkripsi. Pada form Used Own Key, masukkan private key untuk melakukan digital signature. Pada form From/To, masukkan public key milik penerima pesan.
4. Masukkan pesan ke form Message Text, Klik Encrypt. Pesan terenkripsi.
5. Decrypt. Masukkan pesan terenkripsi ke form Encrypted Message. Pada form Used Own Key, masukkan private key untuk mendekripsi pesan. Pada form Sender (Signer's Key), masukkan public key pengirim untuk membuka digital signature di dalam pesan. Klik Decrypt.

Melakukan Verifikasi dengan cara Authentikasi Public Key dengan metode OpenPGP

1. Buka Kleopatra
2. Klik kanan pada certificate yang akan diautentikasi. Pilih Certify Certificate.
3. Centang opsi I have verified the fingerprint. Fingerprint adalah identitas unik dari setiap key, dengan memverifikasi-nya, ini berarti menyatakan bahwa kunci tersebut benar milik orang yang dimaksud
4. Klik Next. Pilih opsi Certify for everyone to see. Klik Certify, masukkan passphrase.
5. Untuk mengecek key tersebut sudah diautentikasi oleh siapa saja, klik kanan pada certificate. Pilih Certificate Detail, buka tab User IDs and Certification.