

MODUL 11

ASYMMETRIC CRYPTOGRAPHY

TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang konsep cryptography PGP
2. Mahasiswa mampu melakukan konfigurasi PGP
3. Mengenalkan mahasiswa tentang konsep digital signature
4. Mengenalkan mahasiswa tentang konsep hash function

DASAR TEORI

A. PGP Secara Umum

PGP adalah suatu metode enkripsi informasi yang bersifat rahasia sehingga jangan sampai diketahui oleh orang lain yang tidak berhak. Informasi ini bisa berupa E-mail yang sifatnya rahasia, nomor kode kartu kredit, atau pengiriman dokumen rahasia perusahaan melalui Internet. PGP menggunakan metode kriptografi yang disebut “public key encryption”: yaitu suatu metode kriptografi yang sangat sophisticated.

PGP menggunakan sistem pasangan kunci privat dan kunci publik. Kunci privat merupakan kunci yang dipegang oleh penggunanya dan tidak boleh diketahui orang lain, sedangkan kunci publik ditujukan untuk publik terutama orang yang akan menerima pesan enkripsi dari seseorang. Enkripsi yang digunakan dalam PGP menggunakan algoritma tertentu. Proses sederhananya adalah anda meng-encrypt pesan dengan kunci publik rekan anda dan kemudian rekan anda membuka pesan ter-encrypt dengan kunci privatnya.

Proses enkripsi cukup memakan waktu dan utilitas CPU, dengan PGP dan algoritma enkripsinya proses ini bisa lebih cepat dengan cara PGP men-encrypt pesan dengan menggunakan kunci publik penerima dan meng-encrypt sebuah kunci pendek untuk meng-encrypt seluruh pesan. Pesan ter-encrypt dengan kunci pendek ini dikirim ke penerima. Penerima akan men-decrypt pesan dengan menggunakan kunci privatnya untuk mendapatkan kunci pendek tadi dan digunakan untuk men-decrypt seluruh pesan.

PGP lahir dua versi kunci publik yaitu Rivest-Shamir-Adleman (RSA) yang dikembangkan sejak 1977 dan Diffie-Hellman. Versi pertama menggunakan algoritma IDEA (International Data Encryption Algorithm) yang dikembangkan di Zurich untuk men-generate kunci pendek dan meng-encrypt seluruh pesan kemudian meng-encrypt kunci pendek tersebut dengan algoritma RSA. Sedangkan versi kedua menggunakan algoritma CAST untuk men-generate kunci pendek dari seluruh pesan untuk meng-encryptnya kemudian menggunakan algoritma Diffie-Hellman untuk meng-encrypt kunci pendek tersebut.

Selain faktor pasangan kunci dan algoritma di atas PGP mempunyai satu lagi fasilitas untuk menyatakan keabsahan dari kunci dan pesan yang terenkripsi yaitu sebuah digital signature (tanda tangan digital). PGP menggunakan algoritma yang efisien untuk men-generate kode hash (kode yang menyatakan integritas sebuah data) dari informasi nama dan informasi lainnya. Hash yang dihasilkan kemudian di-encrypt dengan kunci privat. Penerima kemudian akan menggunakan kunci publik pengirim untuk men-decrypt kode

hash. Jika cocok maka kode hash tadi menjadi digital signature untuk pesan tersebut, sehingga penerima yakin bahwa pesan tersebut dikirim oleh pengirim yang diketahui. PGP versi RSA menggunakan algoritma MD5 (Message Digest 5, 128bit) untuk meng-generate kode hash sedangkan versi Diffie-Hellman menggunakan algoritma SHA-1.

Adapun prinsip kerja dari PGP adalah sebagai berikut :

- PGP menggunakan teknik yang disebut public key encryption dengan dua kode. Kode-kode ini berhubungan secara intrinsik, namun tidak mungkin untuk memecahkan satu sama lain,
- Ketika dibuat satu kunci, maka secara otomatis akan dihasilkan sepanjang kunci, yaitu kunci publik dan kunci rahasia.
- PGP menggunakan dua kunci, Pertama, kunci untuk proses enkripsi (kunci publik). Disebut kunci publik karena kunci yang digunakan untuk enkripsi ini akan diberitahukan kepada umum. Orang yang akan mengirimkan e-mail rahasia kepada kita harus mengetahui kunci publik ini. Kedua, kunci untuk proses dekripsi (kunci pribadi). Disebut kunci pribadi karena kunci ini hanya diketahui oleh kita sendiri.
- Karena dengan conventional crypto, di saat terjadi transfer informasi kunci, diperlukan suatu secure channel. Jika kita memiliki suatu secure channel, mengapa masih menggunakan crypto? Dengan public key system, tidak akan menjadi masalah siapa yang melihat kunci milik kita, karena kunci yang dilihat orang lain adalah yang digunakan hanya untuk enkripsi dan hanya pemiliknya saja yang mengetahui kunci rahasia tersebut.

B. GnuPG

GnuPG adalah software enkripsi email pengganti PGP yang lengkap dan bebas. Bebas karena tidak menggunakan algoritma enkripsi yang telah dipatenkan sehingga bisa dipakai oleh siapa saja tanpa batasan. GnuPG memenuhi spesifikasi OpenPGP RFC2440.

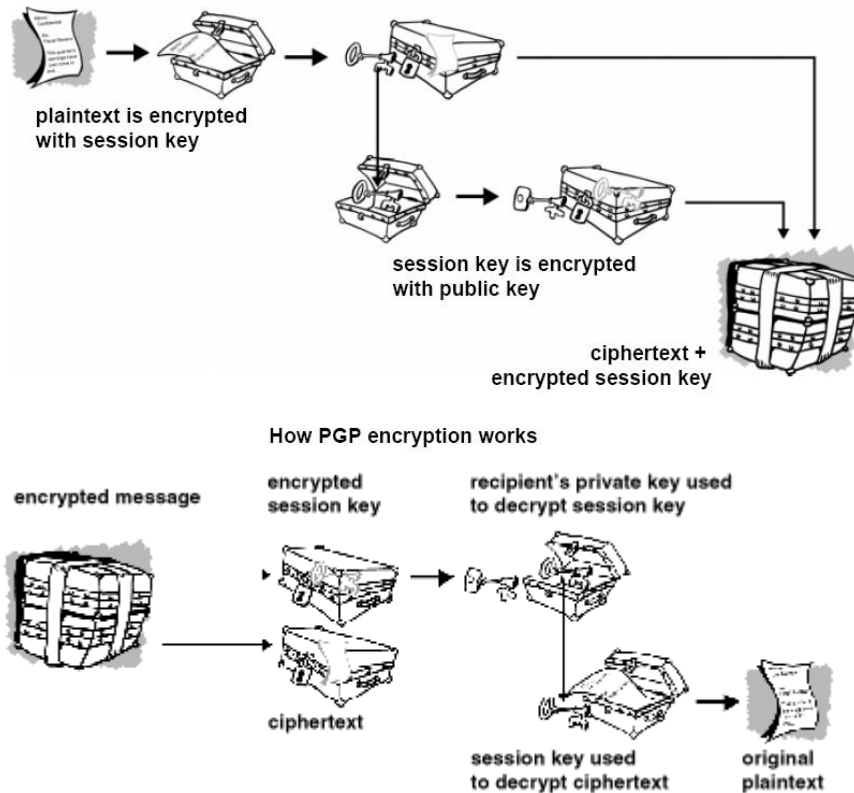
Beberapa fitur yang ditawarkan GnuPG adalah:

- * Penggantian penuh terhadap pemakaian PGP
- * Tidak menggunakan algoritma yang telah dipatenkan
- * Bebas, berlisensi GNU dan ditulis dari awal (from scratch)
- * Fungsi yang lebih baik dibandingkan PGP
- * Kompatibel dengan PGP versi 5 dan yang lebih tinggi
- * Mendukung algoritma ElGamal (signature dan enkripsi), DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 and TIGER.
- * Mudah diimplementasikan jika ada algoritma baru (penggunaan extension modules)
- * Easy implementation of new algorithms using extension modules.
- * Menggunakan format standar untuk identitas user
- * Banyak bahasa yang sudah mentranslasikan
- * Terintegrasi dengan HKP keyservers (www.keys.pgp.net)

GnuPG bekerja sempurna di atas sistem operasi Linux dengan platform x86, mips, alpha, sparc64 ataupun powerpc. Sistem operasi lain dengan platform x86 yang juga bekerja adalah FreeBSD, OpenBSD, NetBSD dan bahkan Windows. Platform lain

dengan sistem operasi selain Linux masih dalam pengembangan.

GnuPG dibuat oleh tim GnuPG yang terdiri dari Matthew Skala, Michael Roth, Niklas Harnaeus, Rmi Guyomarch and Werner Koch. Gael Queri, Gregory Steuck, Janusz A. Urbanowicz, Marco d'Itri, Thiago Jung Bauermann, Urko Lusa and Walter Koch yang membuat translasi resmi dan Mike Ashley yang mengerjakan GNU Privacy Handbook.



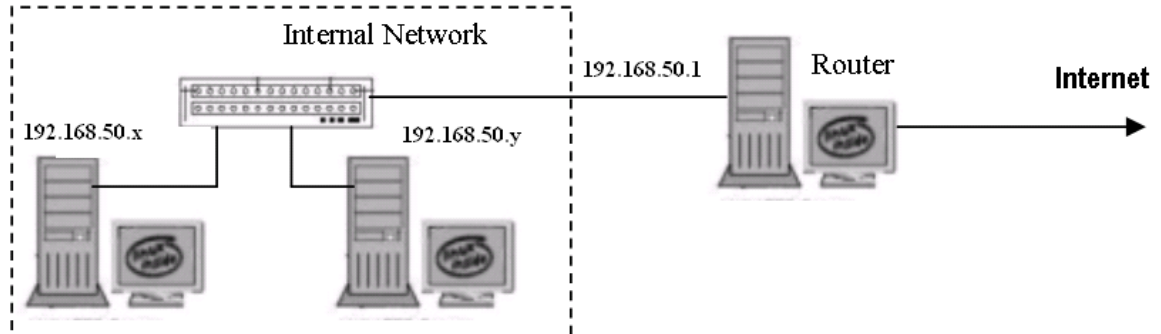
Gambar 1. Cara kerja PGP encryption dan decryption

TUGAS PENDAHULUAN

1. Jelaskan konsep cryptography symmetric dan asymmetric.
2. Keuntungan apa yang diperoleh jika kita menggunakan PGP untuk transfer data.
3. Carilah software aplikasi lainnya untuk proses cryptography baik symmetric maupun asymmetric.

PERCOBAAN

1. Bangunlah jaringan seperti berikut :



Gambar 2 Jaringan Percobaan

NB:

Gunakan dhclient di masing-masing PC untuk mendapatkan IP dari router.

192.168.50.x & y : IP dari router

Pilih 192.168.50.x sebagai PC Server

Pilih 192.168.50.y sebagai PC Client

A. Percobaan dengan asymmetric cryptography

2. Pembuatan kunci (private dan public key) dengan pgp

- a. Pada percobaan ini satu berfungsi untuk mengirim pesan yang terenkripsi (PC Client), dan satunya berfungsi untuk menerima pesan terenkripsi dan melakukan dekripsi terhadap pesan tersebut (PC Server).

Sebelum PC Client mengirim pesan, maka PC Server akan membuat kunci terlebih dahulu, dan mengirimkan public key-nya ke PC Client.

- b. Pastikan FTP Server terinstall pada komputer PC Server.

```
# apt-get install proftpd
```

- c. Pastikan wireshark diinstall pada komputer PC Client

- d. Jalankan wireshark pada komputer PC Client

- e. Pastikan komputer Client dan Server diinstall pgp

```
# apt-get install gnupg
```

- f. Pada komputer PC Server lakukan langkah berikut :

- Lakukan pemilihan algoritma yang digunakan untuk membuat keypair

```
debian:~# gpg --gen-key
gpg (GnuPG) 1.4.9; Copyright (C) 2008 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

```
Please select what kind of key you want:
```

```
(1) DSA and Elgamal (default)
```

```
(2) DSA (sign only)
```

```
(5) RSA (sign only)
```

```
Your selection? 1
```

- Menentukan panjang keypair

```
DSA keypair will have 1024 bits.
```


- Untuk mengetahui kunci public yang sudah dibuat

```

debian:~# gpg --list-keys
/root/.gnupg/pubring.gpg
-----
pub   1024D/14D0B4B3 2009-12-21      => public key
uid                               Muhammad Zen Hadi (Percobaan dengan PGP)
      <zenhadi@eepis-its.edu>
sub   1024g/66715799 2009-12-21      => subkey
NB: 1024D (menggunakan DSA), 1024g (dengan elgamal)
    14D0B4B3 : keyID

```

- Untuk mengetahui kunci privat yang sudah dibuat

```

debian:~# gpg --list-secret-keys
/root/.gnupg/secring.gpg
-----
sec   1024D/14D0B4B3 2009-12-21      => private key
uid                               Muhammad Zen Hadi (Percobaan dengan PGP)
      <zenhadi@eepis-its.edu>
ssb   1024g/66715799 2009-12-21      => subkey

```

3. Proses ekspor kunci public dengan gpg

Sebelum komputer Client mengirim pesan ke komputer Server, maka komputer Server harus mengekspor terlebih dahulu kuncinya ke komputer Client

```

debian:~# gpg --export -a zenhadi@eepis-its.edu
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.9 (GNU/Linux)

mQGIBesvQLURBADuWgukf10ab8H6AhTwtUDx3rIgGn0FKGilzA0/a/xzEV/yULWf
Wc37maXpNMiKY3755Y+mg86K4f2M0x2yFLZLqeQqk7R95bffueKJvkULCPeAsMkb
M4pv8nSMF74fcdXguEr7WAnDNKQe48AiCJyxKsQJehJPn8SGPP1Egl6Z7wCg1sdd
qLIHN11vPDAzvEAbgBHRDqkD/RwA0GueQmsHURDbqLi4rRX6aqkKj/vn5xp6Mdes
VYA9mV44rp6ompOA3N7hrb6Asu15I2+AnWGeM/swoyA6eKJQLJ9rRC//XE+/vw1L
d0qStsH0qY/jVXz2f+sVJk7DxTqafRcHcALoG0I6bh+2RTm9ftzRXeS3hqSHTMiH
4SrrA/0TpVdx9q7y/hrEV2C43tbC0IrKQdHslSd2YZ4VZ1PRHT0e8c1xJdT0A3f
ruVZuph9oIj/avPV/9/FzemLXPv/PoYSfghQmrkVQoo5WVkcUJSRM8i01ErsuKdC
BpJjRerWmCgN6wpd2uF+eZaxk6C01QHwelisJVk0Zv8vYpd9ELRATXVoYw1tYWQg
WmVuIEhhZGkgKFBLCmNvYmFhbiBkZW5nYW4gUEdQKSA8emVuaGFkaUBlZXBpcy1p
dHMuZWR1PohgBBMRagAgBQJLL0C1AhsDBgsJCAcDagQVAggDBBYCAwECHgECF4AA
CgkQjz5B1BTQtL06nACgip74hwf40JAwXyYbCNGSXnrFdSgAoKeMcoyUM/V5xxJh
0aadWZVeAnwtuQENBESvQLUQBACCHI+nDTEqTwNPPDKkvSe0mvgXk8QGw27ykmtE
phHoPTNqhZCJZFfVZgDq376caDZjeHIGLEEsxehqNkTATUGnEHN75e6PrjYe1ruJ
0F3v3vWwNoObKEe9JCxU8XD5SyjRqjM3EZB02gNoCn8mssQWHa9ti02dhBTbXIZg
0S9R1wADBQP+Msgk9jtdrCsytckdPaND+XT7YxMRRIPGvq29zvKXkxmLudQMkwBR
EYkFqy6kzth2XE140nwRRX13QthE0ijVyRI94ZEv+q5XVITClP8udreUgUZB6mIG
463XjS/XGXLVUw65bq5G492rZbKB69YBPvGvv5z5jwWnsv2Wp3TrmKISQQYEQIA
CQUCSy9AtQIbDAACRCRPPKHUFNC0sw+kAJ9RjiUrIh+PfwERzAyOyR8c+W9ACg
qM3ae2XOXreafMPtZWENBGOY6o=
=3ul+
-----END PGP PUBLIC KEY BLOCK-----

```

Note : Agar kunci tersebut bisa dikirim ke komputer Client, bisa disimpan dulu public key-nya dalam sebuah file

```

# gpg --export -a zenhadi@eepis-its.edu > zenhadiPub.asc
-a : menghasilkan output ASCII

```

Untuk mengetahui isi kunci private bisa digunakan perintah :

```
debian:~# gpg --export-secret-keys -a zenhadi@eepis-its.edu
```

4. Proses pengiriman public key

Ketika komputer client ingin mengirim pesan ke komputer server, maka server harus memberikan kunci publiknya terlebih dahulu ke komputer client, bisa dilakukan dengan ftp :

```
debian:~# ftp 10.252.42.99    => no ip dari computer server
Connected to 10.252.42.99.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:10.252.42.99]
Name (10.252.42.99:root): faruq
331 Password required for faruq
Password:
230 User faruq logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get zenhadiPub.asc      => send public key ke computer client
local: zenhadiPub.asc remote: zenhadiPub.asc
200 PORT command successful
150 Opening BINARY mode data connection for zenhadiPub.asc
226 Transfer complete
1377 bytes sent in 0.00 secs (40749.3 kB/s)
ftp> quit
221 Goodbye.
```

5. Proses enkripsi dengan public key dan pengiriman pesan

Pada komputer client, lakukan beberapa perintah berikut ini :

- Import kunci yang sudah dikirim oleh Server.
gpg --import zenhadiPub.asc

NOTE :

Jika di computer client pada waktu mengimport kunci public terdapat error, warp error atau clock in the future, itu artinya jam dan tanggal di computer client tidak matching dengan computer server, dan harus disamakan dulu.

- Cek kunci publik, apakah sudah diterima oleh Client atau belum.
gpg --list-keys
- Buat file text berisi pesan yang akan dikirim ke komputer Server.

```
debian:~# vim coba.txt
Praktikum dengan kriptografi asimetris PGP
```

- Lakukan proses enkripsi terhadap file coba.txt
gpg --encrypt -r zenhadi@eepis-its.edu -a coba.txt
Keterangan :
-a : plain text
-r : recipient

- Hasil enkripsi diatas akan menghasilkan file coba.txt.asc

```
debian:~# cat coba.txt.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.9 (GNU/Linux)

hQE0AysCPq5mcVeZEAP+N1QNYGs7HNIKu+uLa0dWdPQ9nCTIQ50JVHu7bLGop9B2
```

```
fyJu0ky2roewiIwFmsINBAPF4wZeuFUMLYiWJk7hV9zdtxUcniPmBbmMriPwaaZn
ZC6clboh9C3k2SMtNIWQp7X0g00bnYhJNj7N55fBsp0yP8SBrRb57Ekdw97MUVkD
/1FZaCY2JKGLeJ4C4V75uWUuHLYIYAnpUx8SnGb54C1XiATx25cB++rYDs8K3Dd+
7ntosYLDwemai3i7lfjVAC1SitLrS62xZhscbkJEMilXG0y6p6Fiiwa2DNPzpbwX
QshQdoIX9T+QIdRwaGE9dpQa74pfEnG0ibJul950U8C90lEBamLEJdE+lETcCsRH
33i6nSE9DYrQ8V6Cy/YRKdD53KLLZ97fDgH4o4QdYP4JFWw1YmtQutL7wzrIL0VY
GctdADblPINxMCBpk9z0+DskWL8=
=LqAh
-----END PGP MESSAGE-----
```

- Kirim file yang telah dienkripsi tersebut ke komputer tujuan (Server), dengan menggunakan ftp seperti langkah sebelumnya.

6. Proses dekripsi

Pastikan di komputer Server telah menerima pesan yang telah dienkripsi dari komputer client. Lakukan proses dekripsi file tersebut dengan menggunakan private key agar bisa membaca pesan aslinya.

```
debian:~# gpg --decrypt coba.txt.asc

You need a passphrase to unlock the secret key for
user: "Muhammad Zen Hadi (Percobaan dengan PGP) <zenhadi@eepis-its.edu>"
1024-bit ELG-E key, ID 66715799, created 2009-12-21 (main key ID 14D0B4B3)

Enter passphrase:

gpg: encrypted with 1024-bit ELG-E key, ID 66715799, created 2009-12-21
      "Muhammad Zen Hadi (Percobaan dengan PGP) <zenhadi@eepis-its.edu>"
Praktikum dengan kriptografi asimetris PGP => pesan asli
```

7. Berikan kesimpulan awal dari praktikum yang anda lakukan diatas.

B. Percobaan dengan digital signature untuk authentication dan non-repudiation

1. Buat file
vim data.txt
selamat datang di PENS
2. Beri signature pada pesan tersebut dgn private key :
gpg -u 084D3C17 --clearsign data.txt
Note:
084D3C17 sebagai keyID, bisa dilihat dari perintah gpg --list-keys
Dari perintah diatas akan menghasilkan file : data.txt.asc
3. Lihat isi data : data.txt.asc
cat zen.txt.asc

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

selamat datang di PENS
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.6 (GNU/Linux)

iD4DBQFM9oUw+DjcmAhNPBcRAnZ7AKC02ewgwZp+G+dchXFJwSuW/IJ0zQCYotI4
WPB0QNzb30MNB8U7k3SmbQ==
=VP/v
-----END PGP SIGNATURE-----
```

Note :

Pada hasil diatas, terdapat digital signature yang dilekatkan pada pesan aslinya.

4. Untuk mendekrip file diatas gunakan perintah :
gpg --output data --decrypt data.txt.asc

```
gpg: Signature made Thu 02 Dec 2010 12:26:08 AM WIT using DSA key ID 084D3C17
gpg: Good signature from "Muhammad Zen Hadi (Percobaan dengan gpg) <zenhadi@eepi
s-its.edu>"
```

Note :

Hasil diatas untuk membuktikan bahwa pesan diatas memang dikirim dan ditandatangani oleh "Muhammad Zen Hadi".

Dapat juga digunakan perintah :

```
# gpg --verify data.txt.asc
```

5. Untuk melihat data kembali (hasil dari perintah diatas : gpg --output data) :
cat data

C. Percobaan dengan hash function untuk data integrity

1. Buat file :
vim datahash.txt
Selamat datang di kampus PENS, Keputih Surabaya
2. Lakukan perhitungan hash value untuk data diatas :
md5sum datahash.txt
3. Lakukan perubahan isi file datahash.txt, dengan menghilangkan tanda koma
Selamat datang di kampus PENS Keputih Surabaya
4. Hitung kembali hash value :
md5sum datahash.txt
5. Rubah kembali isi file datahash.txt, ganti huruf paling depan dgn huruf kecil
selamat datang di kampus PENS, Keputih Surabaya
6. Hitung kembali hash value :
md5sum datahash.txt
7. Bandingkan hasilnya dari ketiga nilai hash diatas dan apa kesimpulan anda tentang kondisi diatas ?

LAPORAN RESMI

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Simpulkan perbedaan system kriptografi simetris dan asimetris.
3. Berikan satu contoh software aplikasi kriptografi asimetris dan jelaskan penggunaannya.

LEMBAR ANALISA

Praktikum Network Security (Asymmetric Cryptography)

Tanggal Praktikum :

Kelas :

Nama dan NRP :

A. Gambar topologi jaringan beserta dengan IP Addressnya, tunjukkan mana PC Server dan Client

B. Catat hasil pada poin 2.f

a. Pemilihan algoritma

b. Panjang keypair

c. Masa guna keypair

d. Identitas diri

e. Password untuk passphrase

f. Kunci public yang sudah dibuat (gpg --list-keys)

g. Kunci private yang sudah dibuat (gpg --list-secret-keys)

C. Catat hasil pada poin 3 (hanya cukup dituliskan bloknnya saja), contoh :

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1.4.9 (GNU/Linux)

xxxxxxxxxxxxxxxxxx

-----END PGP PUBLIC KEY BLOCK-----

D. Catat pesan plainteksnnya dari poin 5 (coba.txt)

E. Catat hasil enkripsi pada poin 5, tulis seperti di C.

F. Catat hasil dekripsi pada poin 6.

G. Catat hasil dari masing-masing tahapan proses digital signature

a. Poin B.1, B.3, B4 dan B5.

H. Catat hasil dari proses hash function terhadap 3 data yang berbeda