

## PRAKTIKUM KEAMANAN JARINGAN

### MODUL 3

### Email Security

#### TUJUAN PRAKTIKUM:

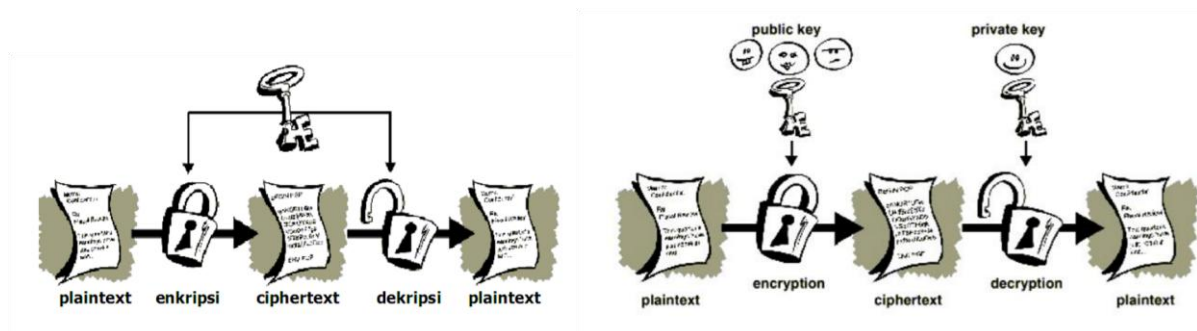
1. Memahami konsep *symmetric* dan *asymmetric cryptography* dalam keamanan email
2. Mampu melakukan *encryption* dan *decryption* email dengan PGP menggunakan Gpg4win
3. Memahami prosedur *authentication* menggunakan metode OpenPGP
4. Mampu mengimplementasikan digital signature pada email

#### DASAR TEORI:

##### PGP Secara Umum

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.



Gbr1. Symmetric Cryptography (ki), Asymmetric Cryptography (ka)

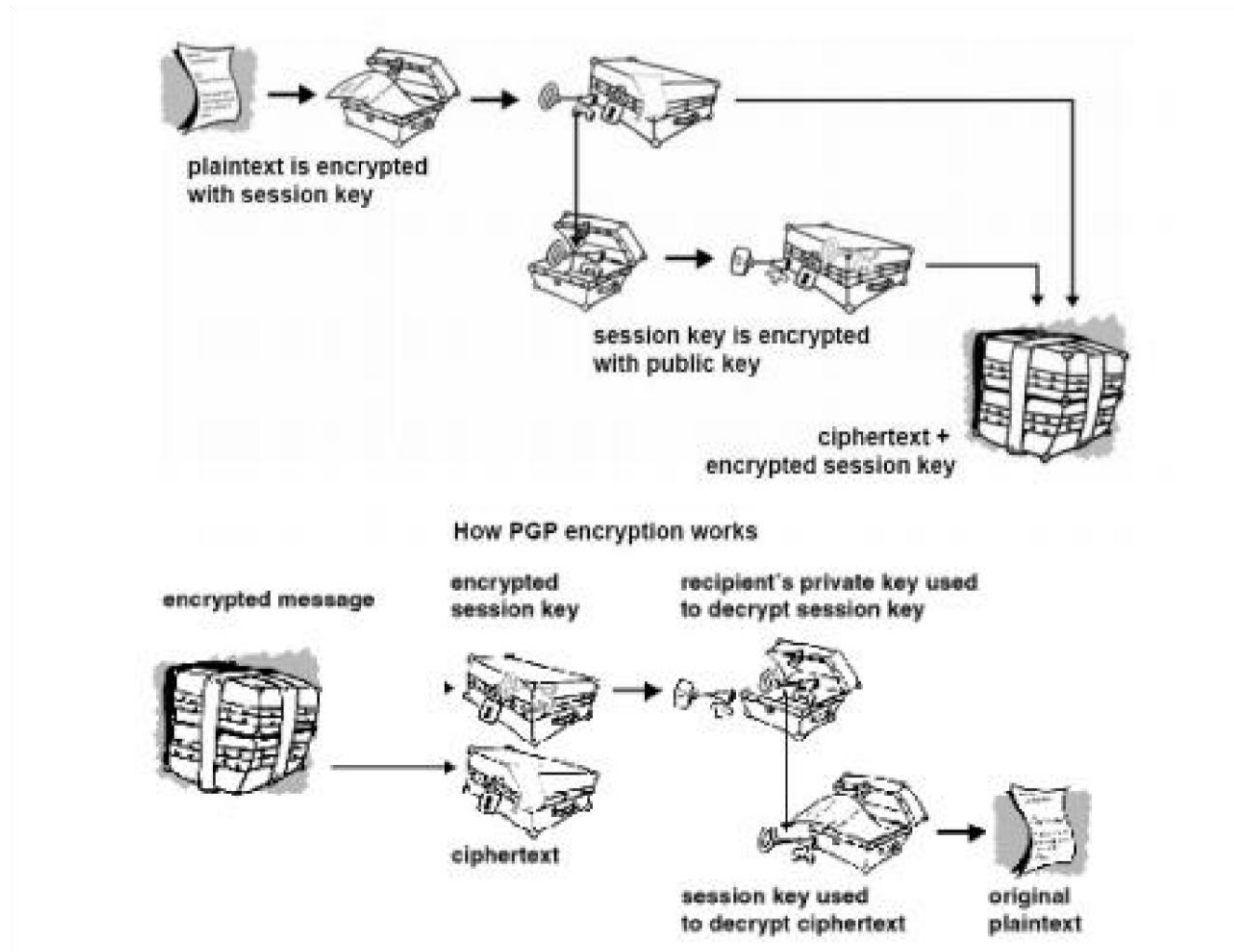
Gpg4win

Gpg4win adalah paket instalasi untuk Windows (2000/XP/2003/Vista/7) dengan program dan handbook untuk enkripsi file dan email. Gpg4win dan program-program di dalamnya adalah *free software*, berbeda dengan software PGP yang berbayar. Gpg4win terdiri dari program-program berikut:

- GnuPG, program inti dari Gpg4win yang bersifat gratis. GnuPG berbasis standar internasional *OpenPGP* (RFC 2440) yang kompatibel dengan PGP serta memiliki infrastruktur yang sama (certificate server, dll). GnuPG versi 2 juga mendukung standar cryptography *S/MIME* (IETF RFC 3851, ITU-T X.509 dan ISIS-MTT/Common PKI)
- Kleopatra, program administrasi certificate yang menyediakan navigasi user untuk semua operasi cryptography maupun pengelolaan key.
- GNU Privacy Assistant (GPA), program alternatif untuk manajemen certificate
- GnuPG for Outlook (GpgOL), extension dari Microsoft Outlook
- GPG Explorer eXtension (GpgEX), extension untuk Windows Explorer
- Claws Mail, program email yang mendukung software GnuPG

Tools lain : Instant Crypt, software opensource untuk melakukan enkripsi & dekripsi berbasis Open PGP

## Encryption - Decryption



## Gbr2. Proses Encryption – Decryption pada PGP/GnuPG

### Authentication

Meskipun memiliki keandalan tinggi, konsep public key ternyata menyisakan masalah dari sisi pengirim pesan. Misalkan Andi dan Budi ingin melakukan korespondensi menggunakan email rahasia. Mereka memang tidak perlu bertemu langsung untuk bertukaran key sebelum berkiriman email rahasia, cukup upload public key di certificate server atau di website masing-masing agar dapat diakses oleh lawan komunikasinya. Namun, bagaimana cara Andi meyakinkan dirinya bahwa public key tersebut adalah benar milik Budi? Dalam kasus tertentu, bisa saja ada orang lain yang berpura-pura menjadi Budi dan menggunakan public key miliknya untuk mendapatkan email rahasia yang seharusnya hanya boleh dibaca oleh Budi. Oleh karenanya, tidak hanya kerahasiaan pesan, tapi identitas dari pemilik public key juga harus terjamin kredibilitasnya. Hal ini disebut dengan authenticity. Terdapat dua metode yang digunakan :

1. S/MIME (Secure/Multipurpose Internet Mail Extension), menggunakan konsep “*hierarchical trust*”. Jika menggunakan S/MIME, public key kita harus diautentikasi terlebih dahulu oleh organisasi terakreditasi sebelum dapat digunakan. Rantai hierarki ini biasanya terdiri dari tiga link : root certificate, certificate authority, dan user certificate
2. OpenPGP, menggunakan konsep “*Web of trust*”. Konsep ini merepresentasikan struktur dasar dari internet non-hierarki beserta user-usernya. Sebagai contoh, jika User B memberikan kepercayaan-nya kepada User A, maka User B juga akan meyakini kebenaran public key milik User C, jika key tersebut sudah diautentikasi kebenarannya oleh User A.



Gbr3. Ilustrasi Public Key yang telah diautentikasi oleh banyak user (konsep Web of Trust)

### Digital Signature

Untuk memastikan bahwa pesan yang diterima adalah benar buatan si pengirim yang kita inginkan, PGP/GnuPG menyediakan fasilitas digital signature atau tandatangan digital. Pengirim menggunakan PGP/GnuPG untuk membuat digital signature dari pesan dengan algoritma RSA atau DSA. Untuk melakukannya, PGP/GnuPG akan melakukan komputasi untuk menghasilkan

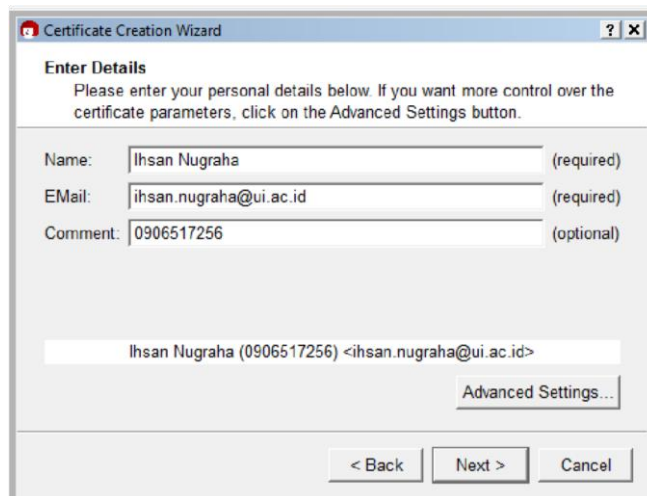
hash (message digest) dari plaintext, dan membuat digital signature dari hasil enkripsi hash tersebut menggunakan private key milik si pengirim.

Penerima kemudian akan menggunakan public key milik si pengirim untuk men-dekripsi kode hash tersebut. Jika cocok, maka kode hash tersebut menjadi digital signature untuk pesan, sehingga penerima yakin bahwa pesan tersebut benar dibuat oleh pengirim yang diketahui, atau belum pernah dimodifikasi oleh siapa pun.

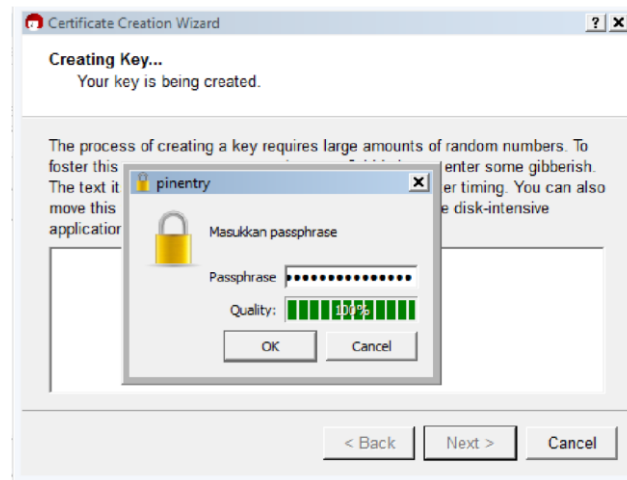
PGP versi RSA menggunakan algoritma MD5 (Message Digest 5, 128 bit) untuk menggenerate kode hash, sedangkan versi Diffie-Hellman menggunakan algoritma SHA-1.

#### Tutorial

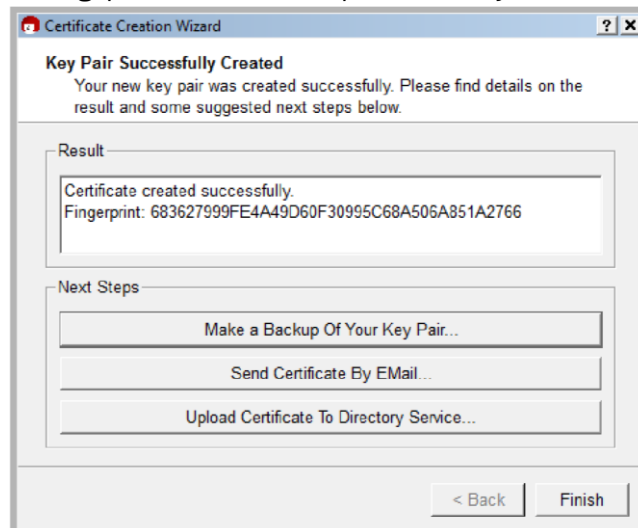
- Membuat Public & Private Key 1. Buka Kleopatra
  2. Klik *File > New Certificate..*
  3. Di kotak dialog, pilih opsi *Create a Personal OpenPGP key pair*
  4. Masukkan detail key



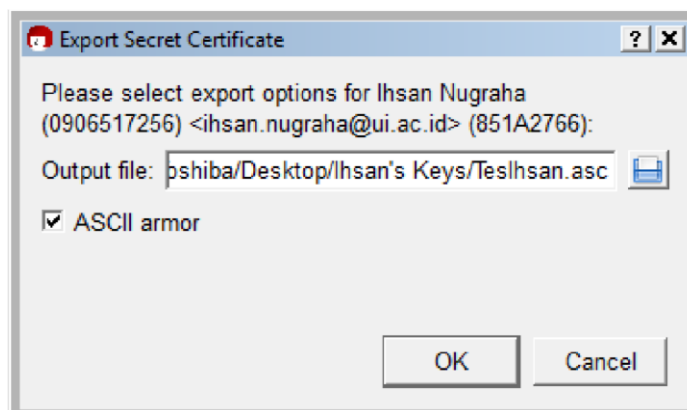
5. Klik *Next > Create Key*, masukkan passphrase. Harus menyertakan karakter angka.



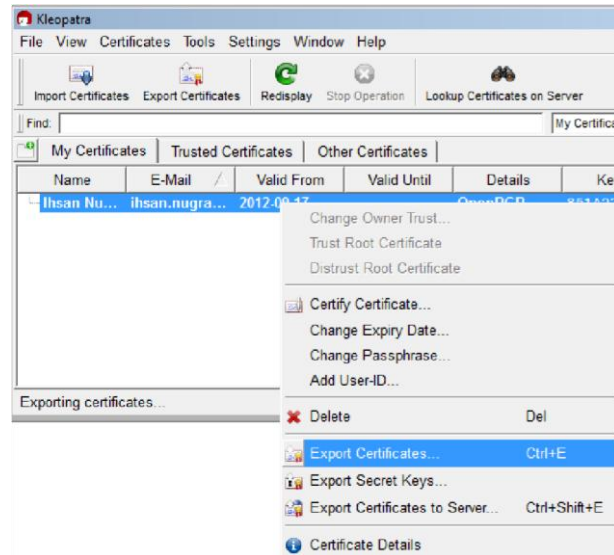
6. Akan muncul kotak dialog, pilih *Make a Backup Of Your Key Pair* untuk meng-export key



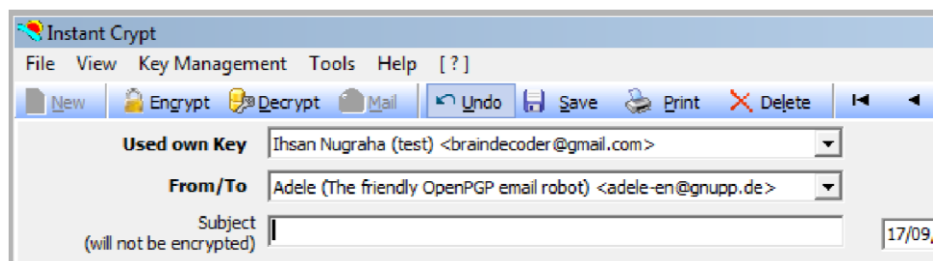
7. Masukkan direktori. Centang opsi *ASCII armor* untuk tipe file \*.asc ; kosongkan untuk tipe file \*.pgp atau \*.pgp.



8. Private key sudah dibuat. Untuk mengexport Public key, klik kanan pada certificate dan pilih *Export Certificate*.

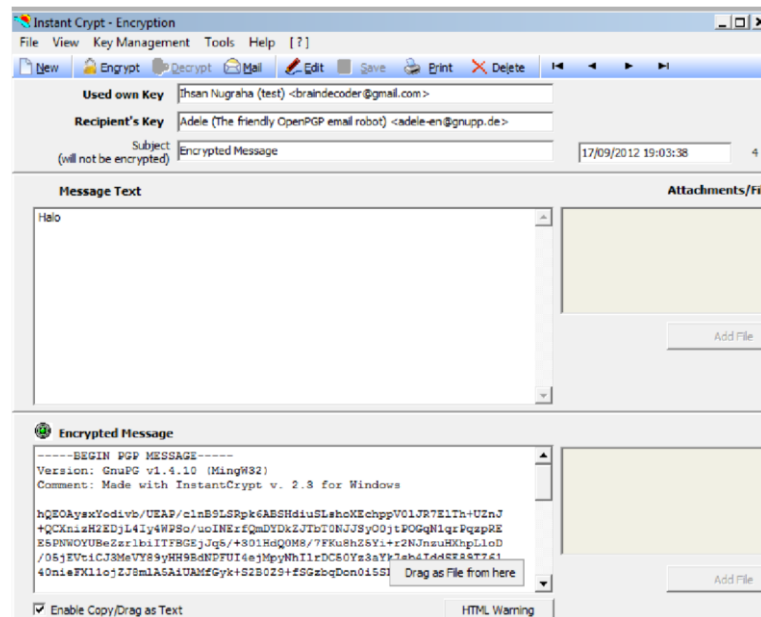


- Melakukan Enkripsi & Dekripsi Pesan
  1. Buka InstantCrypt
  2. Klik *Key Management* > *Import Key* untuk memasukkan key
  3. Enkripsi. Pada form *Used Own Key*, masukkan private key anda untuk melakukan digital signature. Pada form *From/To*, masukkan public key milik penerima pesan.



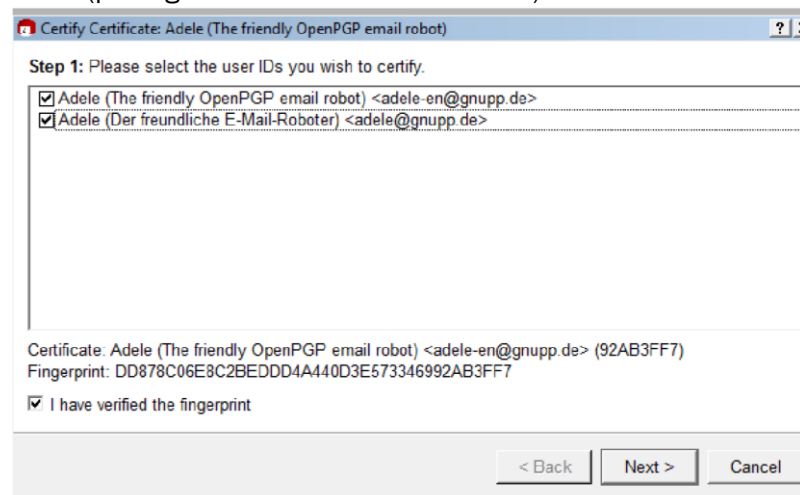
4. Masukkan pesan ke form *Message Text*, Klik *Encrypt*. Pesan terenkripsi.



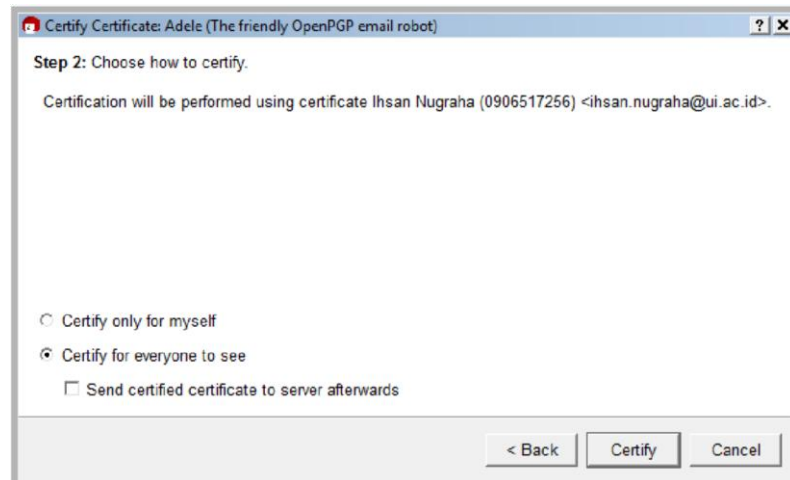


5. Decrypt. Masukkan pesan terenkripsi ke form *Encrypted Message*. Pada form *Used Own Key*, masukkan private key anda untuk mendekripsi pesan. Pada form *Sender (Signer's Key)*, masukkan public key pengirim untuk membuka digital signature di dalam pesan. Klik *Decrypt*.

- Melakukan Autentikasi 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, anda berarti menyatakan bahwa kunci tersebut benar milik orang yang anda maksud (pada gambar di bawah user : Adele)



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*.