UAS

Keamanan Informasi

Disusun oleh:

Boby Dwi Zondi Nata (1410651124)

Kelas : B

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

1. Kriptografi

Pengamanan pesan, data, atau informasi selain bertujuan untuk meningkatkan keamanan, juga berfungsi untuk:

1.Melindungi pesan, data, atau informasi agar tidak dapat dibaca oleh orang-orang yang tidak berhak.

2.Mencegah agar orang-orang yang tidak berhak, menyisipkan atau menghapus pesan, data dan atau informasi. Salah satu hal yang penting dalam komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin kerahasiaan pesan, data, ataupun informasi adalah enkripsi.

Keamanan komputer adalah menjamin data atau informasi tidak dibaca, tidak dimodifikasi oleh orang lain yang tidak diberi otorisasi. Keamanan sistem dibagi menjadi tiga bagian :

1.Keamanan Eksternal

Keamanan eksternal berkaitan dengan fasilitas komputer dari penyusup dan bencana seperti kebakaran atau bencana alam.

2.Keamanan Interface Pamakai

Keamanan interface pemakai yang berkaitan dengan identifikasi pemakai sebelum pemakai diizinkan mengakses data atau program.

3.Keamanan Internal

Keamanan internal berkaitan dengan beragam kendali yang dibangun pada perangkat keras dan perangkat lunak yang menjamin operasi yang handal dan tidak terganngu untuk menjaga integritas data.

Algoritma kriptografi yang baik tidak ditentukan oleh kerumitan dalam mengolah data atau pesan yang akan disampaikan. Yang penting, algoritma tersebut harus memenuhi 4 persyaratan berikut :

1. Privacy / Confidentiality

Inti utama aspek privacy atau confidentiality adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih kearah data-data yang sifatnya privat sedangkan confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluantertentu (misalnya sebagai bagian dari pendaftaran sebuah servis) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

2. Integrity

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi. Sebuah e-mail dapat saja "ditangkap" (intercept) di tengah jalan, diubah isinya (altered, tampered, modified), kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan encryption dan digital signature, misalnya, dapat mengatasi masalah ini.

3.Authentication

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli.

4. Availability

Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi

Salah satu dari bagian kriptografi adalah fungsi hash satu arah. Fungsi hash satu arah adalah dimana kita dengan mudah melakukan enkripsi untuk mendapatkan cipher-nya tetapi sangat sulit untuk mendapatkan plaintext-nya. Salah satu fungsi hash yang paling banyak digunakan adalah Message Digest 5 (MD-5). MD-5 merupakan fungsi hash satu arah yang diciptakan oleh Ron Rivest pada tahun 1991 untuk menggantikan hashfunction sebelumnya. MD-5 adalah salah satu aplikasi yang digunakan untuk mengetahui bahwa pesan yang dikirim tidak ada perubahan sewaktu berada di jaringan. Algoritma MD-5 secara garis besar adalah mengambil pesan yang mempunyai panjang variabel diubah menjadi 'sidik jari' atau 'intisari pesan' yang mempunyai panjang tetap yaitu 128 bit. 'Sidik jari' ini tidak dapat dibalik untuk mendapatkan pesan, dengan kata lain tidak ada orang yang dapat melihat pesan dari 'sidik jari' MD-5. Message digest atau intisari pesan harus mempunyai tiga sifat penting, yaitu :

1.Bila P diketahui, maka MD(P) akan dengan mudah dapat dihitung.
2.Bila MD(P) diketahui, maka tidak mungkin menghitung P.
3.Tidak seorang pun dapat memberi dua pesan yang mempunyai intisari pesan yang sama. H(M) H(M') .

Kriptografi pada dasarnya terdiri dari dua proses, yaitu proses enkripsi dan proses dekripsi. Proses enkripsi adalah proses penyandian pesan terbuka menjadi pesan rahasia (*ciphertext*). *Ciphertext* inilah yang nantinya akan dikirimkan melalui saluran komunikasi terbuka. Pada saat *ciphertext* diterima oleh penerima pesan, maka pesan rahasia tersebut diubah lagi menjadi pesan terbuka melalui proses dekripsi sehingga pesan tadi dapat dibaca kembali oleh penerima pesan.

Elemen Kriptografi

Berikut Elemen-elemen Kriptografi :

Pesan, Plainteks dan Cipherteks.

Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plainteks. Agar pesan tidak bisa dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yan g tersandi disebut cipherteks

Pengirim dan Penerima

Pengirim adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima adalah entitas yang menerima pesan. Entitas di sini dapat berupa orang, mesin (komputer), kartu kredit dan sebagainya.

Enkripsi dan dekripsi

Proses menyandikan plainteks menjadi cipherteks disebut enkripsi. Sedangkan proses mengembalikan cipherteks menjadi plainteks semula dinamakan dekripsi

Cipher

Algoritma kriptografi disebut juga cipher yaitu aturan untuk enciphering dan deciphering, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yaitu himpunan yang berisi elemen-elemen plainteks dan himpunan yang berisi cipherteks. Enkripsi dan dekripsi adalah fungsi yang memetakan elemen-elemen antara kedua himpunan tersebut.

Sistem kriptografi

Sistem kriptografi merupakan kumpulan yang terdiri dari algoritma kriptografi, semua plainteks dan cipherteks yang mungkin dan kunci.

Penyadap

Penyadap adalah orang yang berusaha mencoba menangkap pesan selama ditransmisikan dengan tujuan mendapatkan informasi sebanyak-banyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan maksud untuk memecahkan cipherteks.

Kriptanalisis dan kriptologi

Kriptanalisis (cryptanalysis) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Kriptologi adalah studi mengenai kriptografi dan kriptanalisis.

Metode Kriptografi

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, ciphertext tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali.Proses tranformasi dari plaintext menjadi ciphertext disebut proses *Enciphermen*tatau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali ciphertext menjadi plaintext disebut proses dekripsi (*decryption*). Untuk mengenkripsi dan mendekripsi data. Kriptografi menggunakan suatu algoritma (cipher) dan kunci (key). Cipher adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi data. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data.

Jenis-jenis algoritma kriptografi :

Algoritma kriptografi adalah algoritma yang berfungsi untuk melakukan tujuan dari ilmu kriptografi itu sendiri. Algoritma kriptografi terdiri dari 2 bagian fungsi, yaitu :

- ENKRIPSI (encryption) Proses tranformasi dari plaintext menjadi ciphertext disebut proses*Encipherment* atau enkripsi (*encryption*).
- DEKRIPSI (decryption). Proses mentransformasikan kembali ciphertext menjadi plaintext disebut proses dekripsi (*decryption*).

Secara umum berdasarkan kesamaan kuncinya, algoritma sandi dibedakan menjadi :

ALGORITMA KUNCI SIMETRIS.

Dalam symmetric cryptosystem ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai *secret-key ciphersystem*. Kriptografi *secret key* seringkali disebut sebagai kriptografi konvensional atau kriptografi simetris (*Symmetric Cryptography*) dimana proses dekripsi adalah kebalikan dari proses enkripsi dan menggunakan kunci yang sama. Kriptografi simetris dapat dibagi menjadi dua, yaitu penyandian blok dan penyandian alir. Penyandian blok bekerja pada suatu data yang terkelompok menjadi blok-blok data atau kelompok data dengan panjang data yang telah ditentukan. Pada penyandian blok, data yang masuk akan dipecah-pecah menjadi blok data yang telah ditentukan ukurannya. Penyandian alir bekerja pada suatu data bit tunggal atau terkadang dalam satu byte. Jadi format data yang mengalami proses enkripsi dan dekripsi adalah berupa aliran bit-bit data. Algoritma yang ada pada saat ini kebanyakan bekerja untuk penyandian blok karena kebanyakan proses pengiriman data pada saat ini menggunakan blok-blok data yang telah ditentukan ukurannya untuk kemudian dikirim melalui saluran komunikasi.

ALGORITMA KUNCI ASIMETRIS.

Algoritma Asimetris atau sering disebut algoritma public key, penggunaan kunci dalam algoritma ini adalah, kunci yang dipakai dalam proses enkripsiberbeda dengan kunci yang dipakai pada proses dekripsi, jadi jumlah kunci enkripsi ≠ kunci dekripsi.

Ada 2 jenis kunci di algoritma ini, yaitu

1. **KUNCI PUBLIK** adalah kunci yang digunakan untuk melakukan proses enkripsi data. Kunci ini disebut publik karena siapapun dapat mengetahuinya.

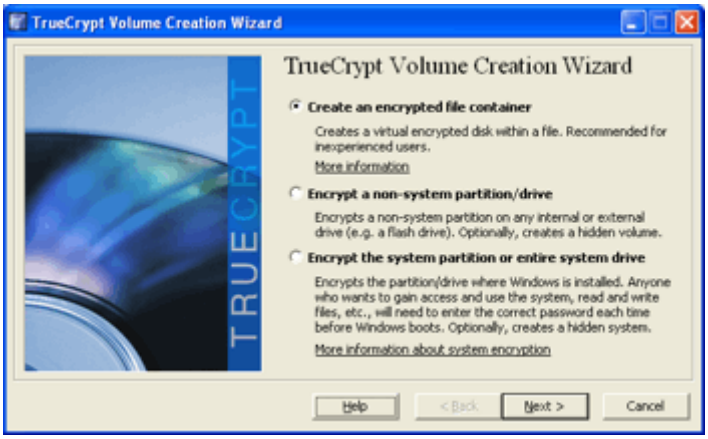
2. **KUNCI PRIVAT** adalah kunci yang digunakan untuk melakukan proses dekripsi data. Kunci ini disebut privat karena 1 kunci privat hanya dimiliki oleh 1 orang saja. Kunci privat sering juga disebut kunci rahasia.

Istilah kunci rahasia dalam algoritma simetris digunakan untk menyatakan kunci enkripsi dan dekripsi, sementara pada algoritma asimetris digunakan untuk menyatakan kunci privat, karena kunci publik tidak dirahasiakan.

2. **Enkripsi data rahasia dengan menggunakan TrueCrypt**
   Pertama kali kita harus membuat sebuah wadah tempat penyimpanan data rahasia kita yang disebut *TrueCrypt Volume*. TrueCrypt Volume ini bisa kita simpan dalam sebuah file (*container*), partisi atau hardisk secara keseluruhan. Untuk mulai menggunakan TrueCrypt Volume ini kita harus me-*mount*-nya menjadi sebuah *virtual drive*. Dan setelah selesai digunakan jangan lupa untuk men-d*ismount* kembali virtual drive tersebut, sehingga orang lain tidak bisa mengakses data-data kita.

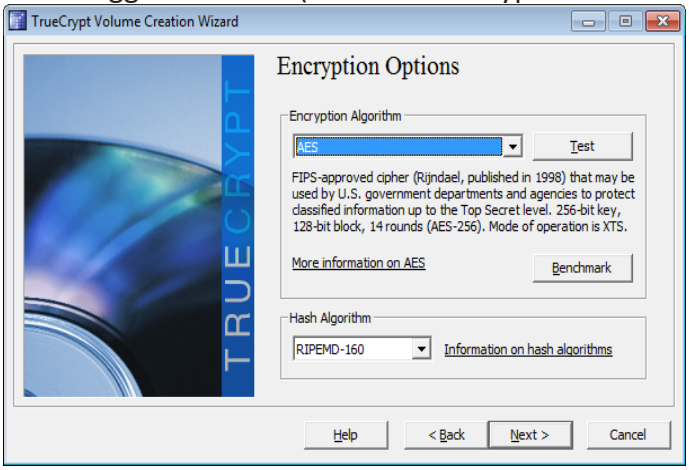
   Dalam contoh dibawah ini, saya akan membuat sebuah *TrueCrypt Volume* pada sebuah file. Jadi orang lain hanya bisa melihat file tersebut tanpa menyadari bahwa sebenarnya didalam file tersebut tersimpan data-data yang kita miliki.

1. Install dan jalankan aplikasi TrueCrypt selanjutnya klik Create Volume.
2. Pada jendela TrueCrypt Volume Creation Wizard, kita harus memilih dimana TrueCrypt Volume akan dibuat. Karena kita akan meyimpan volume TrueCrypt ini pada sebuah file, maka pilih opsi pertama “create an encrypted file container”, lalu klik Next.

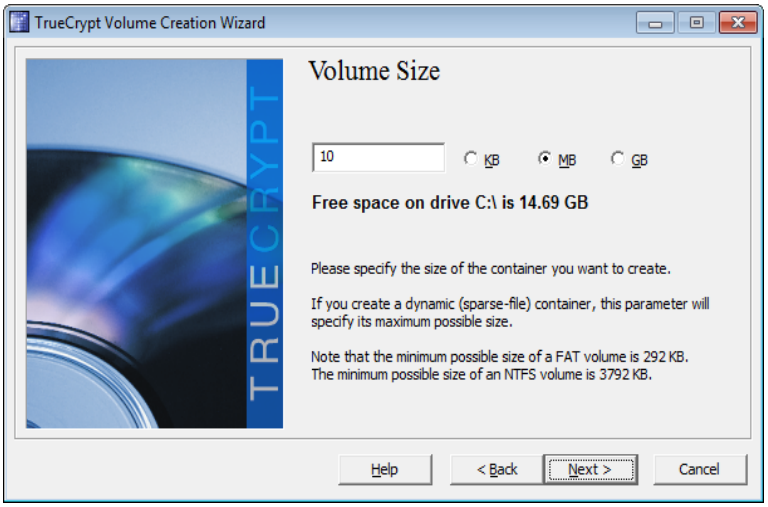


3. Tentukan tipe volume yang akan dibuat, secara default pilih "Standard TrueCrypt volume" lalu klik *Next*.
4. Langkah selanjutnya adalah menentukan lokasi tempat penyimpanan file. Dalam contoh ini kita akan meyimpan TrueCrypt Volume pada file yang saya beri nama PRIVATE yang berlokasi di C:\DATAKU, pastikan sebelumnya folder DATAKU sudah dibuat, klik Next untuk melanjutkan.

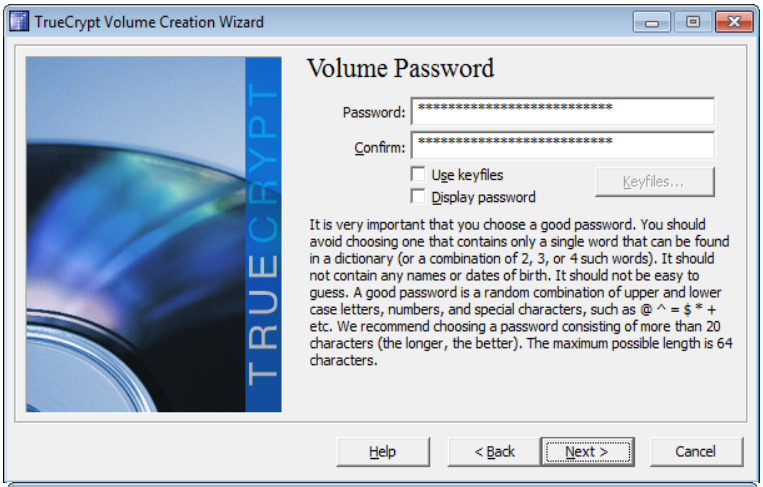
5. Pada jendela Encryption Options, klik aja *Next* untuk memilih Algoritma Enkripsi secara default yaitu menggunakan *AES* (Advanced Encryption Standard).

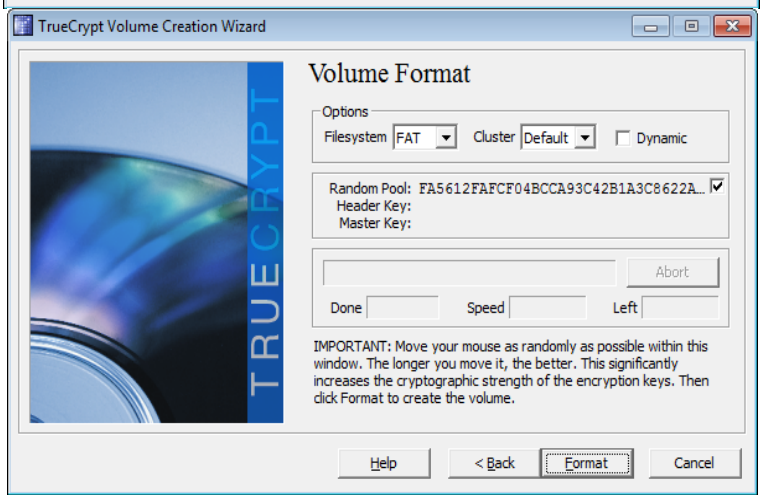


6. Selanjutnya pada jendela Volume Size tentukan besarnya volume yang akan kita buat, misalnya sebesar 10 MB.

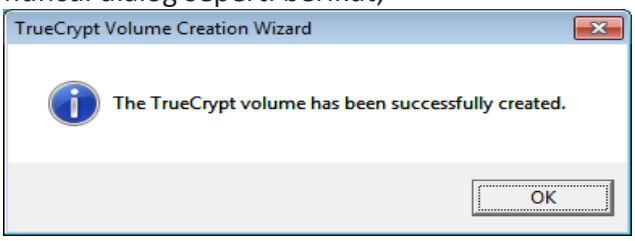


7. Langkah selanjutnya masukkan Password, kemudian Format volume tersebut, klik Next dan Finish.

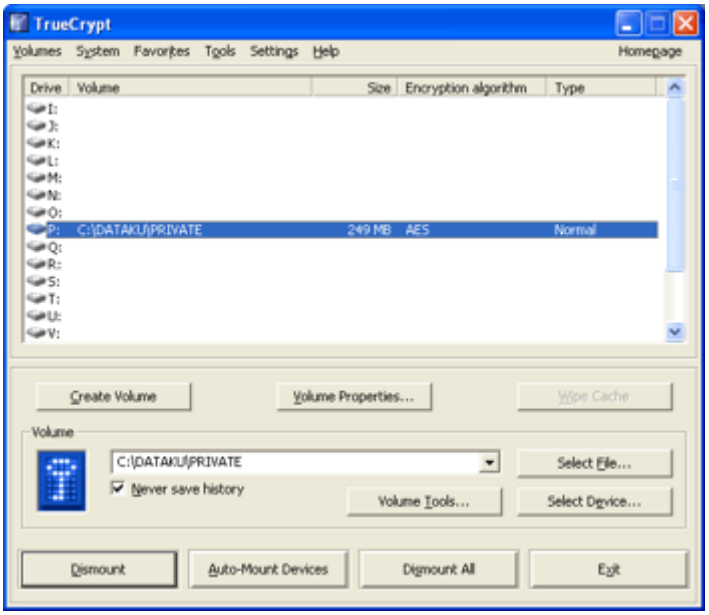




8. Jika berhasil akan muncul dialog seperti berikut;



9. Untuk memulai menggunakan volume tersebut sebagai penyimpanan data, langkah selanjutnya adalah me-mount volume tersebut menjadi virtual drive. Jalankan kembali aplikasi TrueCrypt, pilih drive letter yang kita sukai, misal klik drive P.
10. Selanjutnya klik Select File untuk memilih encrypted file container yang telah kita buat, yaitu file PRIVATE pada folder C:\DATAKU
11. Klik Mount, masukan password yang telah kita buat pada langkah no 7 dan klik OK, sebuah virtual drive P akan terbentuk, klik Exit.



12. Simpan data-data rahasia kita ke drive ini, ingat ukurannya tidak bisa melebihi volume size yang telah kita buat pada langkah no 6.
13. Setelah selesai digunakan, dismount kembali virtual drive tersebut dengan cara jalankan kembali aplikasi TrueCrypt, pilih virtual drive P, klik Dismount.

Demikianlah cara sederhana untuk melindungi data rahasia menggunakan aplikasi TrueCrypt