

BAB I

PENDAHULUAN

1.1 Latar Belakang

Data dapat menjadi salah satu aset penting dalam kelangsungan hidup perusahaan mana pun. Penyimpanan data memerlukan berbagai macam pertimbangan, terutama dari segi keamanannya. Penggunaan *laptop/notebook* saat ini menimbulkan masalah baru berkaitan dengan penyimpanan data tersebut. Mau tidak mau, perusahaan harus mengizinkan data penting mereka “berkeliaran” di luar. Untuk menyelesaikan masalah ini, enkripsi data sebaiknya dilakukan.

Teknik enkripsi yang umum digunakan adalah enkripsi yang dilakukan pada file atau *file encryption*. Satu file yang diinginkan dienkripsi pada satu waktu. *File encryption* sudah dilakukan bertahun-tahun dan masih memiliki manfaat dari segi keamanan. Namun, *file encryption* juga memiliki kekurangan terutama apabila dihadapkan pada kondisi tertentu. Misalnya, jika *file* yang berisi informasi penting berjumlah banyak, seperti *file-file* yang dimiliki oleh suatu perusahaan. *File encryption* yang dilakukan membutuhkan penanganan yang baik berkaitan dengan status *file* apa yang dienkripsi menggunakan kunci apa.

Disk encryption merupakan alternatif enkripsi data selain *file encryption*. Enkripsi ini disebut juga enkripsi volume (*volume encryption*). Penggunaan kata volume dikarenakan enkripsi ini seakan-akan dilakukan pada area tertentu. Area itu menjadi sebuah volume/ kontainer yang dapat digunakan untuk menyimpan *file-file* penting. Berdasarkan besarnya volume tersebut, *disk encryption* dapat digolongkan menjadi dua yakni *entire hard disk encryption (EHD encryption)* dan *virtual hard disk encryption (VHD encryption)* [REF04].

Sesuai namanya, *EHD encryption* berarti enkripsi dilakukan pada seluruh area *hard disk*, termasuk faktor yang menyangkut perangkat keras *hard disk* itu sendiri. Dengan demikian, *EHD encryption* ini hanya dapat diimplementasikan secara khusus terhadap salah satu jenis *hard disk* tertentu. Jenis enkripsi ini tentu memiliki kelebihan karena seluruh area *hard disk* aman. Namun, jika dikaitkan dengan jaringan dan kegiatan

sharing yang biasa dilakukan di dalamnya, *EHD encryption* menuntut penyesuaian yang tidak mudah.

VHD encryption, di sisi lain, tidak melakukan pengamanan terhadap seluruh area *hard disk*, tetapi hanya sebagian. Dengan demikian, sepanjang ada kesesuaian sistem enkripsi dengan sistem operasi tempat *VHD encryption* terinstal, semua akan berjalan lancar, tidak perlu memikirkan faktor yang berkaitan dengan perangkat keras *hard disk*. Karena kelebihan pada aspek tersebut, topik tugas akhir ini menggunakan sistem enkripsi ini.

Mengenai cara kerja *VHD encryption*, pada dasarnya, sistem ini mengizinkan pengguna untuk membuat sebuah *file volume*, yaitu sebuah file yang menyimpan konfigurasi dan data *disk* yang terenkripsi. Sebuah *virtual disk* akan dimunculkan jika pengguna memberikan *password* yang tepat untuk membuka *file volume* tadi. *Virtual disk* yang muncul tidak berbeda dengan *disk* biasa, dapat digunakan untuk menyimpan *file*. *File* yang tersimpan di dalamnya pun dapat diperlakukan seperti layaknya bila tersimpan pada *disk* yang lain, yakni dapat di-*copy*, di-*paste*, di-*delete*, dan sebagainya. Satu perbedaan antara *virtual disk* ini dengan *disk* biasa adalah seluruh data yang disimpan pada *disk* ini secara otomatis dan transparan akan dienkripsi.

Pada saat melakukan enkripsi terhadap data yang disimpan di dalamnya, *disk encryption* bekerja dengan blok bit. Oleh karena itu untuk membangun sistem enkripsi seperti ini, algoritma enkripsi yang dipakai adalah algoritma yang bekerja dengan blok bit juga. Jenis algoritma seperti itu dinamakan *cipher* blok (*block cipher*). Rangkaian bit plainteks/cipherteks yang akan dienkripsi atau didekripsi dibagi menjadi blok-blok bit yang panjangnya sama dan sudah ditentukan sebelumnya[MUN04].

Banyak algoritma kriptografi cipher blok yang sudah pernah dipublikasikan. Untuk menyebut beberapa di antaranya adalah *DES(Data Encryption Standard)*, *Triple DES(3DES)*, *IDEA(International Data Encryption Algorithm)*, *Blowfish*, *Gost*, *Safer*, *LOKI*, *FEAL*, *RC2*, *RC5*, *Serpent*, dan lain-lain [MUN04]. Salah satu algoritma kriptografi *cipher* blok yang terbaru adalah algoritma Rijndael. Algoritma ini adalah pemenang sayembara terbuka yang diadakan oleh *NIST (National Institute of Standards and Technology)* untuk membuat standard algoritma kriptografi yang baru

sebagai pengganti *Data Encryption Standard (DES)*. DES sudah dianggap tidak aman terutama karena panjang kunci yang relatif pendek sehingga mudah dipecahkan menggunakan teknologi saat ini. Standard tersebut diberi nama *Advanced Encryption Standard (AES)*. Tepatnya pada bulan November 2001, algoritma Rijndael ditetapkan sebagai *AES*, dan diharapkan Rijndael menjadi standard kriptografi yang dominan paling sedikit selama 10 tahun [MUN04]. Kenyataan bahwa algoritma Rijndael merupakan algoritma kriptografi *cipher* blok yang masih baru dan belum dinyatakan tidak aman adalah dasar pemilihan algoritma ini menjadi algoritma enkripsi pada topik tugas akhir ini. Alasan lain untuk memilih algoritma Rijndael adalah algoritma ini sudah terbukti dapat diimplementasikan untuk aplikasi *disk encryption*.

Pembangunan sebuah perangkat lunak *disk encryption* sejak awal didasarkan pada pilihan-pilihan komponen yang membentuknya. Dengan jenis *virtual hard disk encryption*, algoritma Rijndael, perangkat lunak *disk encryption* yang dibangun diharapkan dapat memberikan faktor keamanan yang cukup kuat sambil menjaga performansi tetap tinggi dan dapat digunakan secara luas. Komponen lain yang perlu dipertimbangkan dalam implementasi *disk encryption* ini adalah sistem operasi yang digunakan. *Microsoft Windows* yang sudah dikenal luas menjadi pilihan sistem operasi untuk implementasi *disk encryption* ini.

1.2 Rumusan Masalah

Rumusan masalah yang dijadikan dasar pengerjaan tugas akhir ini meliputi:

1. Bagaimana membuat *virtual disk* pada sistem operasi *Windows*.
2. Bagaimana mengenkripsi *virtual disk* dengan algoritma Rijndael.

1.3 Tujuan

Tujuan utama dan tujuan pendukung tugas akhir ini adalah sebagai berikut:

- a. Memahami konsep *disk encryption* dan perbedaannya dengan *file encryption*.
- b. Memahami algoritma Rijndael.
- c. Memahami dan mengimplementasikan cara pembuatan *virtual disk* pada sistem operasi *Windows*.
- d. Mengimplementasikan *disk encryption* dengan algoritma Rijndael.
- e. Menguji keamanan untuk disk yang telah dienkripsi

1.4 Batasan Masalah

Yang menjadi batasan masalah dalam pelaksanaan tugas akhir ini adalah implementasi yang dilakukan tidak memberikan solusi keamanan terhadap segala perlakuan yang dikenakan pada *file volume*, terutama penghapusan terhadap *file* tersebut.

1.5 Metodologi

Dalam penyusunan tugas akhir ini akan digunakan metodologi sebagai berikut:

1. Studi Literatur

Studi literatur akan dilakukan pada seluruh proses pengerjaan Tugas Akhir. Studi literatur meliputi studi tentang *disk encryption* dan algoritma Rijndael. Studi literatur juga dilakukan pada cara pembuatan *virtual disk* pada sistem operasi *Windows*. Literatur yang digunakan dapat berupa buku, artikel ilmiah, maupun situs web.

2. Analisa kebutuhan perangkat lunak

Kegiatan analisa perangkat lunak meliputi analisa spesifikasi perangkat lunak, analisa lingkungan pengembangan, analisa fungsionalitas, dan analisa kelas.

3. Perancangan perangkat lunak

Perancangan perangkat lunak meliputi perancangan kelas, dan perancangan antarmuka.

4. Implementasi

5. Pengujian perangkat lunak

Pengujian dilakukan untuk menemukan dan memperbaiki bug-bug yang ada. Pengujian juga dilakukan menyangkut tingkat keamanan *disk* yang terenkripsi.

6. Perbaikan

Perbaikan dilakukan terhadap kesalahan-kesalahan yang mungkin terjadi pada program, laporan, dan dokumentasi teknis.

1.6 Sistematika Pembahasan

Sistematika pembahasan tugas akhir ini adalah sebagai berikut:

1. BAB I – Pendahuluan
Bab pendahuluan membahas mengenai latar belakang penulisan tugas akhir, rumusan persoalan, tujuan tugas akhir, ruang lingkup dan batasan yang diacu, metodologi yang digunakan serta sistematika pembahasan.
2. BAB II – Dasar Teori
Bab dasar teori memuat berbagai pengetahuan yang didapat melalui studi literatur. Pengetahuan yang dibahas meliputi konsep *disk encryption*, jenis *disk encryption*, konsep *virtual disk* yang akan digunakan dan algoritma Rijndael.
3. BAB III – Analisis dan Perancangan
Bab ini memuat analisis kebutuhan dan perancangan perangkat lunak yang akan dikembangkan dalam Tugas Akhir ini.
4. BAB IV – Implementasi dan Pengujian
Bab ini mencakup detail implementasi perangkat lunak yang dikembangkan dalam Tugas Akhir dan berbagai pengujian yang dilakukan terhadap perangkat lunak yang dikembangkan beserta hasil pengujiannya.
5. Bab V – Penutup
Bab ini berisi kesimpulan pelaksanaan Tugas Akhir serta saran penggunaan dan pengembangan perangkat lunak lebih lanjut.