STUDI FITUR *BITLOCKER DRIVE ENCRYPTION* PADA *MICROSOFT WINDOWS VISTA*

Anthony Rahmat S. – NIM : 13506009

Program Studi Teknik Informatika,
Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16009@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang studi fitur *BitLocker Drive Encryption* pada sistem operasi *Microsoft Windows Vista*. Fitur ini dibuat dengan tujuan untuk meningkatkan keamanan data bahkan sebelum komputer melakukan *booting* terhadap sistem operasi. *BitLocker Drive Encryption* mampu mengamankan data pada komputer dengan melakukan proses enkripsi-dekripsi secara menyeluruh pada drive komputer, sesuai dengan namanya, *Drive Encryption*.

BitLocker Drive Encryption memiliki tiga mode operasi, yaitu *Transparent Operation Mode, User Authentication Mode,* dan *USB Key Mode*. Ketiga jenis mode operasi ini menentukan bagaimana *BitLocker Drive Encyption* dioperasikan. Tingkat keamanan yang ditawarkan setiap mode implementasi berbeda-beda. Masing-masing model implementasi *BitLocker Drive Encryption* memiliki kelebihan dan kekurangan tersendiri. *BitLocker* menggunakan media penyimpanan eksternal sebagai media penyimpan kunci. Media tersebut dapat berupa media storage USB maupun sebuah chip bernama *Trusted Platform Module (TPM)*. Sebagai algoritma, *BitLocker Drive Encryption* menggunakan *AES (Advanced Encryption Standard)*.

***Kata kunci**: BitLocker Drive Encryption, Microsoft Windows Vista, booting,* enkripsi, dekripsi, USB, *Trusted Platorm Module, Advanced Encyption Standard*.

1. Pendahuluan

Faktor keamanan pada komputer merupakan salah satu aspek yang perlu diperhatikan seiring dengan berkembangnya teknologi informasi. Kenyamanan dan kemudahan yang didapatkan dari peran teknologi informasi dalam kehidupan manusia tidak berarti tanpa jaminan privasi atau keamanan bagi para penggunanya. Oleh karena itu banyak dikembangkan perangkat-perangkat lunak yang khusus diciptakan untuk menangani masalah keamanan ini.

Perkembangan perangkat lunak, tidak terkecuali sistem operasi pada komputer, dari waktu ke waktu selalu membawa perubahan ke arah yang lebih baik, terutama jika dilihat dari aspek keamanan data pada komputer. Untuk menjamin tidak terjadinya pencurian data atau perbuatan ilegal sejenisnya, berbagai sistem operasi saat ini ditambahkan fitur-fitur yang khusus diciptakan untuk menangani masalah keamanan data dengan algoritma kriptografi tertentu. Salah satu dari sistem operasi tersebut adalah sistem operasi buatan *Microsoft* yang masih tergolong baru, yaitu *Windows Vista*. *Windows Vista* bahkan memiliki fitur tambahan untuk menunjang terjaminnya keamanan data yang tidak ditemukan pada versi-versi *Windows* sebelumnya. Fitur tersebut bernama *BitLocker Drive Encryption*.

2. *TPM (Trusted Platform Module)* sebagai *chip* penyimpan kunci

BitLocker Drive Encryption menggunakan media eksternal sebagai media penyimpanan kunci. Media eksternal tersebut dapat berupa *Trusted Platform Module (TPM)* dan media storage eksternal seperti *USB Flash Disk* atau *External Hard Disk*. TPM adalah sebuah *microchip* yang terintegrasi dengan *motherboard* komputer dan sifatnya unik pada setiap *motherboard* yang berbeda. Secara garis besar, TPM memiliki fungsionalitas khusus untuk menangani aspek keamanan komputer melalui kriptografi. Namun terkait aplikasi *BitLocker Drive Encryption*, TPM hanya dilibatkan sebatas penyimpan kunci saja. Selain itu, perlu diketahui bahwa TPM termutakhir saat ini adalah TPM dengan versi 1.2 atau lebih.

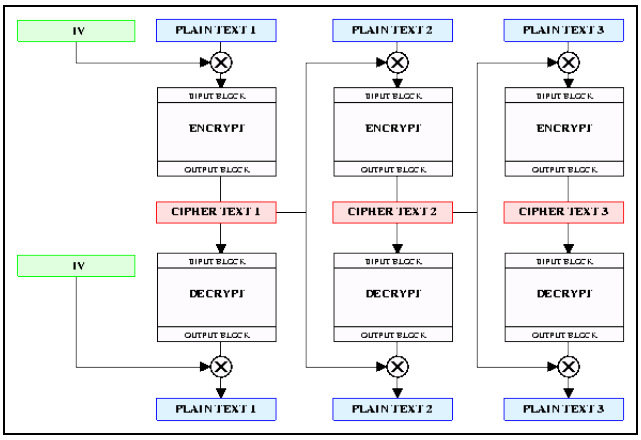
3. Algoritma Kriptografi pada *BitLocker Drive Encyption*

Secara umum, *BitLocker* menggunakan algoritma jenis kriptografi kunci simetri. Algoritma yang dipakai dalam pengoperasian enkripsi dan dekripsi terhadap kunci-kuncinya adalah AES *(Advanced Encryption Standard)*. Sebenarnya, algoritma-algoritma lain seperti *RSA* dan *SHA256* juga terlibat, namun pemakaiannya tidak dominan seperti AES.

Algoritma AES yang akan dipakai dapat dipilih sesuai keinginan pengguna. Berikut pilihan algoritma AES beserta length yang tersedia:

1. AES 128-bit
2. AES 256-bit
3. AES 128-bit + Diffuser
4. AES 256-bit + Diffuser

Mode operasi blok yang digunakan pada algoritma *AES* adalah *Cipher Block Chaining* (*CBC*).



Gambar 1. Enkripsi-Dekripsi pada Algoritma Kunci Simetri dengan Operasi CBC

4. Cara Kerja *BitLocker Drive Encryption*

Perlu diketahui terlebih dahulu bahwa sebenarnya *BitLocker* tidak mengenkripsi seluruh sektor pada *drive* harddisk, melainkan menyisakan sedikit bagian dari *drive* tersebut. Segmen tersebut adalah yang menyimpan segala informasi untuk melakukan *booting* ke sistem operasi yang terinstal pada komputer (dinamakan *bootmanager*). *Bootmanager* tidak boleh dienkripsi karena akan dijalankan pertama kali ketika komputer dinyalakan.

BitLocker juga menyediakan fasilitas *Integrity check*. *Integrity check* adalah rangkaian pemeriksaan terhadap semua modul yang dijalankan ketika komputer dinyalakan (dimulai dari *bootmanager* sampai *OS Loader*). Hal ini bertujuan untuk memastikan bahwa tidak ada manipulasi *environment* sistem ketika *booting* dilakukan. Salah satu manfaat dari *Integrity Check* adalah mencegah kerja *virus boot sector* (virus yang bekerja sebelum komputer melakukan *boot* ke sistem operasi).

Enkripsi dan dekripsi tidak lepas dari pengguaan kunci, begitu juga dengan aplikasi *BitLocker*. Berikut ini nama kunci-kunci yang digunakan beserta penjelasannya:

1. FVEK (*Full Volume Encryption Key*)
   FVEK adalah kunci yang digunakan langsung untuk mendekripsi seluruh isi *volume/drive*, sesuai namanya, *Full Volume*. Kunci ini memiliki *length* bervariasi antara 128-bit dan 256-bit. FVEK tidak dapat dilihat oleh user karena tersimpan di dalam sektor harddisk tertentu sebagai *metadata* dan dalam keadaan terenkripsi. Untuk itu, FVEK harus didekripsi terlebih dahulu dengan menggunakan VMK sebelum dapat digunakan sebagai kunci dekripsi volume. Algoritma yang digunakan untuk mendekripsi FVEK adalah AES + CBC.

2. VMK (*Volume Master Key*)
   VMK adalah kunci untuk mendekripsi FVEK (FVEK yang masih tersimpan dalam keadaan terenkripsi). Panjang kunci ini adalah 256-bit. Jika VMK terbongkar, pendekripsian FVEK akan dapat dilakukan dengan mudah. Oleh karena itu, VMK adalah kunci yang paling krusial dalam aplikasi *BitLocker*. Sama seperti FVEK, VMK tersimpan dalam keadaan terenkripsi di sektor tertentu harddisk sebagai *metadata* sehingga tidak dapat dilihat oleh pengguna. VMK hanya dapat didekripsi oleh salah satu dari SRK, SK dan RK, atau Clear Key tergantung dari mode operasi *BitLocker* yang dipilih user.

3. SRK (*Storage Root Key*)
   SRK adalah kunci yang sekaligus menjadi identitas unik TPM. Sebenarnya, SRK adalah kunci publik pada algoritma RSA, di mana kunci privatnya selalu tersimpan dan tidak pernah dimunculkan oleh chip TPM. Panjang kunci ini adalah 2048-bit, mengingat setiap perangkat TPM memiliki kunci publik (SRK) yang berbeda. SRK tersimpan di dalam TPM dalam bentuk plainteks, tidak terenkripsi.

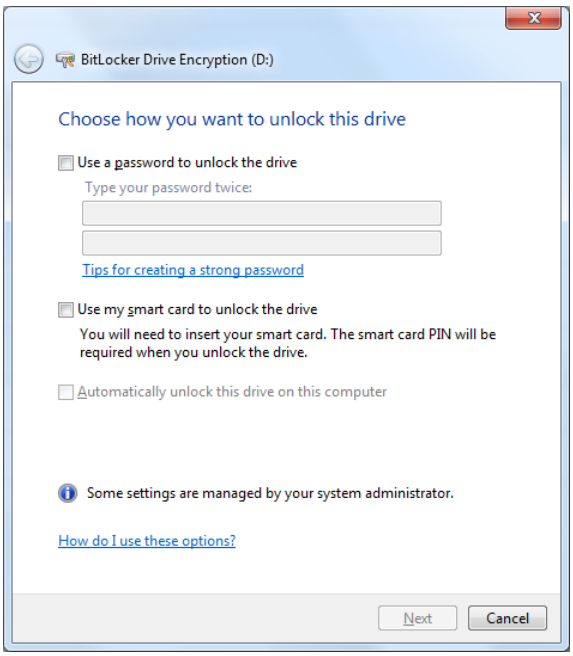
4. SK (*Startup Key*)
   SK adalah kunci yang hanya ada (dibangkitkan) jika pengguna memilih mode operasi tertentu pada

BitLocker. Kunci ini tersimpan di media penyimpanan eksternal seperti USB Flash Disk. SK memiliki length 256-bit.

5. RK (R*ecovery Key*)
   RK adalah kunci yang hanya ada jika SK ada. Sama seperti SK, kunci ini tersimpan di media penyimpanan eksternal. RK memiliki length yang sama dengan SK yaitu 256-bit. Sesuai namanya, RK berperan sebagai "kunci cadangan" jika SK hilang.

6. Clear Key
   Kunci ini hanya dibangkitkan oleh *BitLocker* jika pengguna tidak menggunakan media eksternal sama sekali (termasuk TPM) dalam mengoperasikan *BitLocker*. Dengan kata lain, Clear Key hanya ada jika SK, RK, dan SRK tidak ada. Clear Key memiliki panjang karakter 256-bit. Clear Key tersimpan dalam keadaan tidak terenkripsi dan di tempat yang sama seperti VMK dan FVEK sehingga tidak dapat dilihat oleh user.

Keenam kunci di atas dibangkitkan secara acak ketika fitur *BitLocker Drive Encryption* pada *Windows Vista* di-*enable*. Mengenai kunci yang mana yang akan digunakan untuk mendekripsi VMK, apakah SRK, SK/RK, atau Clear Key, ditentukan berdasarkan mode operasi yang dipilih pengguna *BitLocker*.



Gambar 2. Pemilihan mode operasi

Hampir keseluruhan kerja *BitLocker* dilakukan pada lingkungan *pre-boot*, yaitu ketika komputer belum melakukan *booting* terhadap sisten operasi tertentu. Pada dasarnya, *BitLocker* memiliki tiga mode operasi, yaitu mode operasi transparan, autentikasi pengguna, dan mode perangkat USB. Ketiga operasi ini adalah

1. Mode Transparan (*TPM-only*)
   Chip TPM digunakan dalam mode ini. Prinsip utama dari mode ini adalah bagaimana membuat pengguna komputer agar seakan-akan tidak menyadari bahwa sebenarnya *drive* pada komputernya terenkripsi. Dengan kata lain, tidak ada *user input* apapun untuk dapat melakukan *boot* ke sistem operasi. Berikut ini adalah prosedur yang dilakukan dalam mode transparan:
   a. Ketika komputer dinyalakan, *Integrity Check* dilakukan.
   b. Setelah lolos, *BitLocker* memindahkan SRK dari TPM ke modul memori (RAM) untuk pemakaian selanjutnya.
   c. SRK digunakan untuk mendekripsi VMK dengan algoritma AES + CBC.
   d. VMK yang telah terdekripsi digunakan untuk mendekripsi FVEK dengan algoritma yang sama.
   e. FVEK digunakan untuk mendekripsi *drive*, lalu sistem operasi dapat segera di-*boot*

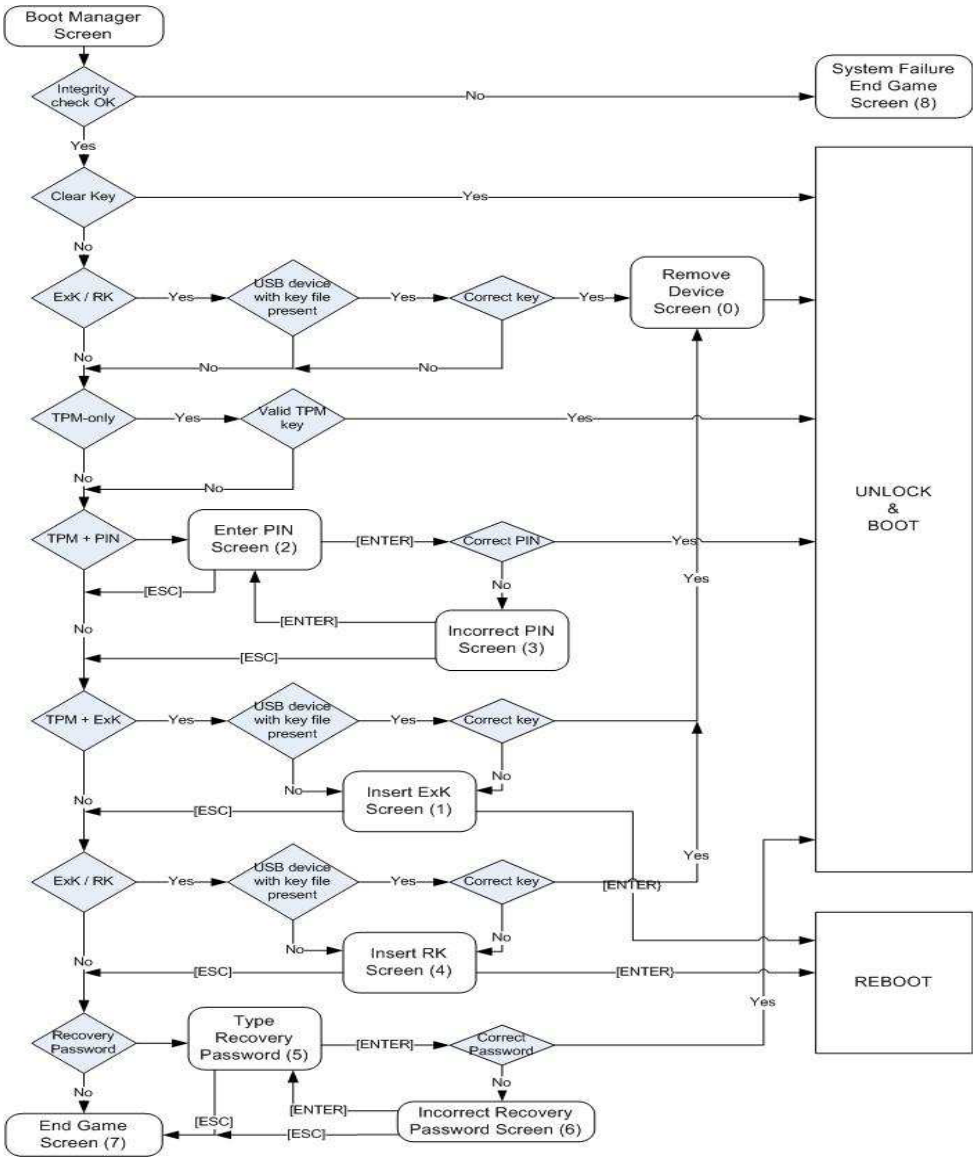
2. Mode Autentikasi Pengguna (*TPM+PIN* atau *TPM+SK/RK*)
   Mode ini adalah mode transparan yang memerlukan input dari user sebagai autentikasi sebelum melakukan *booting* (TPM juga digunakan). Autentikasi dapat dilakukan dengan dua cara, yaitu dengan PIN yang diinput langsung oleh pengguna , dan dengan media USB yang didalamnya tersimpan SK atau RK. Berikut ini adalah prosedur yang dilakukan dalam mode autentikasi pengguna:
   a. *Integrity Check* dilakukan ketika komputer dinyalakan.
   b. Setelah lolos, *BitLocker* mengambil SRK dari TPM.
   c. Jika pengguna menggunakan PIN, maka sebuah kunci yang berupa (SRK+SHA256(PIN)) harus dibuat terlebih dahulu untuk kemudian digunakan untuk mendekripsi VMK dengan algoritma AES + CBC.
   d. Jika pengguna menggunakan media USB, maka sebuah kunci yang berupa (XOR(SRK(IK),SK)) harus dibuat terlebih dahulu untuk kemudian digunakan untuk mendekripsi VMK dengan

algoritma AES + CBC. IK di sini adalah *Intermediate Key*, yaitu sebuah kunci 256-bit yang dibangkitkan secara random bersamaan ketika SK atau RK dibangkitkan.

e. Setelah VMK didapat, selanjutnya FVEK didekripsi dengan cara yang sama, lalu sistem operasi di-*boot*

3. Mode Perangkat USB (*SK/RK-only*)
Mode ini adalah mode jika komputer tidak memiliki perangkat TPM. Media penyimpanan eksternal digunakan sebagai pengganti TPM. Prosedurnya adalah sebagai berikut:

a. *Integrity Check* dilakukan ketika komputer dinyalakan.
b. Setelah lolos, *BitLocker* mengambil SK dari media USB (atau RK jika SK tidak ditemukan).
c. SK atau RK digunakan sebagai kunci untuk mendekripsi VMK dengan algoritma AES+CBC
d. Setelah VMK didapat, selanjutnya FVEK didekripsi dengan cara yang sama, lalu sistem operasi di-*boot*



Gambar 3. Cara Kerja *BitLocker Drive Encryption*

5. Kelebihan *BitLocker Drive Encryption*

BitLocker Drive Encryption sebagai salah satu aplikasi yang menggunakan prinsip *Full-Disk Encryption*, memiliki keuntungan diantaranya sebagai berikut:

1. Semua jenis partisi dari volume harddisk dapat dienkripsi secara menyeluruh. Namun, partisi yang berjenis *Master Boot Record* (atau yang berisi kode-kode *bootstrap*) tidak dapat dienkripsi karena MBR adalah partisi yang dibutuhkan oleh komputer untuk dapat melakukan *booting* ke sistem operasi tertentu. Seluruh partisi selain MBR dapat dienkripsi.
2. *Full Disk Encryption* berarti seluruh data ataupun file yang berada pada volume/partisi harddisk akan terenkripsi tanpa terkecuali. Hal ini dapat dikatakan sebagai suatu keuntungan dengan mempertimbangkan sisi pengguna. Keuntungan dari sisi pengguna di sini maksudnya adalah agar tidak lagi terjadi kelalaian pengguna terhadap data-data penting yang lupa terenkripsi karena enkripsi dilakukan langsung terhadap satu *drive harddisk*. Pengguna komputer tidak perlu lagi mengenkripsi file satu per satu.
3. *BitLocker Drive Encryption* menawarkan metode-metode autentikasi yang berbeda bagi pengguna untuk dapat kembali mengakses *drive-drive* yang terenkripsi. Semua metode autentikasi pada dasarnya sama, yaitu tetap dilakukan secara *pre-boot*, yang berarti autentikasi pengguna dilakukan sebelum pengguna "masuk" ke sistem operasi yang dituju. Metode-metode autentikasi pada fitur ini adalah autentikasi dengan USB (*Universal Serial Bus*) Flash Disk, nomor atau sandi privat (PIN), dan autentikasi secara transparan. Ketiga metode tersebut dapat dipilih sesuai keinginan pengguna.
4. Tingkat keamanan yang sangat tinggi. Tingginya tingkat sekuriti dari fitur ini dapat dilihat dari perlindungan data yang langsung diterapkan pada satu *drive*, bukan dalam satuan *file*, sehingga akan menjadi sangat sulit untuk membongkar isi file yang berada pada *drive* yang sedang terenkripsi.

6. Celah Keamanan pada *BitLocker Drive Encryption*

Enkripsi yang diterapkan langsung pada *drive*, bukan pada satuan *file*, membuat keamanan *BitLocker Drive Encryption* sangat sulit untuk ditembus karena seluruh konten drive yang sudah dienkripsi akan menjadi *scrambled*, atau dengan kata lain baik nama file maupun struktur direktori sudah tidak dapat terbaca lagi. Sampai saat ini, belum ditemukan cara untuk dapat membongkar isi drive yang sudah "acak" seperti yang telah disebutkan.

Dibalik tingginya tingkat keamanan yang ditawarkan oleh *BitLocker Drive Encryption*, masih ada cara untuk membobolnya. Metode yang sudah cukup terkenal adalah *cold-boot attack*. Prinsip utama dari *cold-boot attack* adalah dengan memanfaatkan komponen modul memori atau RAM *(Random Access Memory)* pada motherboard dan media penyimpan kunci kriptografi (dalam hal ini dapat berupa *TPM* atau *USB Flash Disk*). Seperti yang sudah disebutkan sebelumnya, bahwa pendekripsian *drive* dilakukan tepat sebelum sistem operasi melakukan *booting* sistem operasi. Pendekripsian tersebut memerlukan kunci kriptografi pada media penyimpanan kunci sehingga modul memori pada sistem komputer harus memiliki salinan kunci tersebut untuk kepentingan pemakaian selanjutnya. *Cold-boot attack* memanfaatkan mekanisme seperti ini untuk mendapatkan kunci.

Sebelum melakukan *cold-boot attack*, ada beberapa persiapan yang harus terpenuhi, diantaranya:

1. Media penyimpanan data eksternal (seperti *USB Flash Disk* atau *External Hard Disk Drive*) yang di dalamnya sudah terinstal sistem operasi tertentu (biasanya menggunakan Linux) yang dapat di-*boot* langsung dari media tersebut.
2. Komputer yang ingin "diserang" tidak sedang dalam pengawasan pemiliknya karena metode ini tidak dapat dilakukan jika komputer tersebut sedang digunakan oleh pemiliknya.

Secara garis besar, prosedur *cold-boot attack* adalah sebagai berikut:

1. Pasang media eksternal yang sudah terinstal sistem operasi yang *bootable* di dalamnya sebelum komputer target dinyalakan.
2. Nyalakan komputer, lakukan pengaturan BIOS (jika perlu) agar komputer melakukan *boot* terhadap sistem operasi yang ada di media eksternal yang terpasang. Karena sistem operasi yang akan di *boot* tidak berada di media storage (harddisk) internal komputer, maka *BitLocker Drive Encryption* tidak akan menanyakan kunci dekripsi.
3. Setelah sistem operasi berhasil di *boot* dengan baik, segera matikan komputer dengan "paksa" (tanpa melakukan prosedur *shutdown*).
4. Ambil modul memori atau RAM pada motherboard untuk pencarian kunci selanjutnya (pencarian kunci pada RAM tidak akan dibahas pada makalah ini).

Dengan melakukan prosedur di atas, bukan berarti kunci kriptografi sudah pasti berhasil ditemukan. Hal ini disebabkan oleh kemampuan RAM yang terbatas untuk tetap dapat mempertahankan data yang berada di dalamnya tanpa kehadiran arus listrik. Sampai saat ini, RAM hanya dapat mempertahankan datanya sampai beberapa menit saja jika tidak dialiri arus listrik.

Prosedur *cold-boot attack* di atas dapat diantisipasi dengan menambahkan autentikasi pengguna tepat setelah komputer dinyalakan. Tujuannya adalah agar tidak sembarang orang dapat melakukan *booting* ke *operating system* sehingga langkah nomor 2 pada prosedur di atas dapat dicegah. Selain itu, pengguna juga disarankan untuk selalu melakukan *shutdown* setiap kali ingin mematikan komputer untuk mengosongkan RAM dan agar *BitLocker Drive Encryption* dapat kembali mengenkripsi *drive*.

Kesimpulan

BitLocker Drive Encryption adalah solusi yang sangat baik untuk mengatasi persoalan keamanan data pada komputer. Dari sisi keamanan data, aplikasi ini memiliki tingkat kesulitan yang tinggi untuk dibobol sebagai hasil dari penggunaan algoritma AES + CBC dan prinsip *full disk encryption*. Nilai yang sangat baik juga dicapai jika dilihat dari segi kepraktisan karena pengguna tidak perlu repot lagi untuk mengenkripsi *file* satu per satu yang memungkinkan adanya *file* yang lupa untuk dienkripsi.

Daftar Referensi

[1] Microsoft. Explore the features: BitLocker Drive Encryption
http://www.microsoft.com/windows/windows-vista/features/bitlocker.aspx
Tanggal akses 12 Maret 2009 pukul 15.00 WIB

[2] TechRepublic. Prevent data theft with Windows Vista's Encrypted File System (EFS) and BitLocker
http://articles.techrepublic.com.com/5100-10878_11-6162949.html
Tanggal akses 11 Maret 2009 pukul 21.00 WIB

[3] Wikipedia. Advanced Encryption Standard
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Tanggal akses 11 Maret 2009 pukul 20.00 WIB

[4] Wikipedia. Full Disk Encryption
http://en.wikipedia.org/wiki/Full_disk_encryption
Tanggal akses 11 Maret 2009 pukul 20.00 WIB

[5] Microsoft. BitLocker Drive Encryption Security Policy
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp947.pdf
Tanggal akses 25 Maret 2009 pukul 15.00 WIB