# Penerapan Kriptografi Pada Perangkat Digital Book Reader (DigiReader) Untuk Kelestarian Lingkungan

Ecko Manalu – 13508604
Program Studi Teknik Informatika
Institut Teknologi Bandung
Jl Ganesha 10, Bandung 40116
E- Mail : ecko_mnl@yahoo.com, if18604@students.if.itb.ac.id

## Abstrak

Penggunaan kertas sebagai bahan pencetakan utama buku-buku hingga saat ini seperti tidak bisa tergantikan. Telah dicoba usaha untuk membuat versi digital dari semua buku seperti novel, komik, dan sebagainya, dengan tujuan untuk mengurangi penggunaan kertas dalam proses pencetakan, namun hal tersebut menghadapi masalah dalam hal hak cipta. Karena dengan mudahnya orang akan dapat menggandakan buku digital tersebut sehingga dapat merugikan para penulis buku. Tulisan ini berisi suatu pengajuan untuk membuat suatu perangkat yang disebut DigiReader, suatu perangkat keras yang dapat membaca buku digital, yang bertindak sebagai pengganti buku cetak, yang di dalamnya terdapat proses kriptografi baik di aras perangkat keras maupun aras perangkat lunak. Tulisan ini bisa dikatakan masih suatu rancangan kasar untuk menuju ke arah tersebut, dan masih membutuhkan pengembangan berikutnya.

Kata Kunci *: Buku digital, kriptografi, kriptografi aras perangkat keras, kriptografi aras perangkat lunak.*

**Latar Belakang**

Hingga saat ini kertas merupakan bahan utama dalam pembuatan buku. Fakta yang tertulis pada sebuah publikasi oleh *id2Communications* dalam *Facts about Paper and Paper Waste* [ID2] yang dirangkum dari berbagai sumber terpercaya, 2 milyar buku, 359 juta majalah, dan 24 milyar surat kabar dicetak setiap tahunnya di Amerika. Angka tersebut diperoleh masih untuk satu negara Amerika Serikat, belum termasuk ratusan negara lainnya di Dunia. 2 milyar buku tiap tahunnya di Amerika tersebut jika dianggap berisi paling sedikit 100 lembar, maka bisa dikatakan sebanyak 200 milyar lembar kertas dicetak setiap tahunnya. Fakta berikutnya dalam publikasi tersebut adalah jika dikonversi menjadi pohon yang menjadi bahan utama pembuatan kertas, maka 35% penebangan pohon di seluruh dunia akan dapat dihindarkan jika kita tidak lagi menggunakan kertas sebagai media, hal tersebut berlaku untuk buku juga. [ID2]

Lama telah dicetuskan, bahwa pembuatan buku versi elektronik atau disebut e-book, memang merupakan suatu solusi untuk menanggulangi masalah lingkungan tersebut. Namun

masalah baru sekaitan dengan hak cipta muncul setelah e-book ini diterapkan. Hal ini muncul karena dengan adanya e-book, proses penggandaan atau pembajakan buku menjadi semakin cepatnya, sehingga bisa merugikan pihak-pihak yang memegang hak cipta terhadap buku tersebut. Meskipun saat ini telah dilakukan berbagai macam cara untuk menghindari pembajakan e-book tersebut, baik peningkatan dari segi enkripsinya, proteksi dokumen, dan lainnya, namun tetap saja pembajakan itu dapat tetap dengan mudah dilakukan hanya dengan bantuan satu tombol Print Screen.

**Rumusan Masalah**

Dua masalah yang telah diuraikan di atas yakni masalah pelestarian lingkungan dan pembajakan merupakan masalah utama yang akan diselesaikan dalam makalah ini.

**Pendekatan Penyelesaian**

Kriptografi merupakan suatu solusi yang ditawarkan dalam upaya untuk menyelesaikan masalah ini. Kriptografi yang selama ini hanya populer di sisi perangkat lunak, akan diterapkan juga dalam sisi perangkat keras.

**Landasan Teori**

**Kriptografi**

Definisi lama : Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. [MUN01]

Kriptografi berkembang sehingga tidak lagi sebatas mengenkripsi pesan tapi juga memberikan aspek keamanan yang lain. [MUN01]

Kriptografi oleh Schneier didefinisikan sebagai ilmu sekaligus seni untuk menjaga keamanan pesan.

Kebutuhan akan kriptografi ini semakin meningkat seiring dengan semakin meningkatnya kesadaran masyarakat akan keamanan data, serta semakin tingginya frekuensi pengiriman data melalui berbagai media komunikasi serta banyak kebutuhan lainnya. Salah satunya yang akan disoroti dalam hal ini adalah mengenai perlindungan terhadap hak cipta.

**Kriptografi dalam aras perangkat keras**

Melalui pengertian dipaparkan di atas dapat dikembangkan bahwa segala upaya untuk menjaga keamanan pesan dapat digolongkan sebagai kriptografi. Lebih jauh lagi, dapat dikatakan bahwa Kriptografi bukan hanya dapat dilakukan dengan bantuan perangkat lunak pemrograman saja seperti kebanyakan yang diketahui saat ini. Pendekatan kriptografi dengan perangkat keras pun sebenarnya termasuk dalam ruang lingkup kriptografi.

Ide mengenai penggunaan perangkat keras untuk mengamankan peredaran arsip lagu baik itu audio maupun mp3, telah sukses dilakukan oleh perusahaan Macintosh lewat sistem penjualan lagu iTunes. iPod memang merupakan suatu pemutar musik yang portabel layaknya pemutar musik yang beredaran di pasaran saat ini, namun perangkat keras ini memiliki kelebihan yang hingga kini diakui oleh dunia sangat sulit untuk ditembus keamanannya (dibaca datanya). Tidak mudah untuk melakukan transfer data dari dan ke iPod ini, jika tidak menggunakan iTunes. Kondisi

inilah yang pada akhirnya memberi perlindungan yang tinggi untuk setiap karya musik.

Ide penggunaan sebuah perangkat keras khusus untuk melindungi pesan yang ada di dalamnya seperti iTunes ini menjadi suatu bukti bahwa adalah sangat mungkin untuk melakukan enkripsi data dalam aras perangkat keras.

Produk harddisk yang dapat dienkripsi secara real-time telah dikeluarkan oleh produsen khusus media penyimpanan data, diantaranya *Seagate* dan *SecureD*. Proses enkripsi dan dekripsi dilakukan dengan memanfaatkan suatu alat yang disebut dengan *SmartCard*. Metode ini akan digunakan dalam skema enkripsi dan dekripsi yang diajukan dalam tulisan ini. [ASD1,SAF1]

Dalam proses kriptografi di aras perangkat lunak, ada yang disebut dengan cipher block, penggunaan jaringan feistel, serta banyak jenis lainnya. Sebenarnya operasi yang dilakukan dalam proses kriptografi ini adalah operasi yang sebenarnya dilakukan dalam gerbang logika, seperti contohnya : XOR, *shifting*, dan sebagainya.

Pemaparan di atas adalah suatu studi mengenai bahwa kriptografi bukan hanya mungkin dilakukan di aras perangkat lunak namun juga di aras perangkat keras.

**Kriptografi dalam aras perangkat lunak**

Mengenai Kriptografi dalam aras perangkat lunak telah banyak dikembangkan selama ini. Berbagai algoritma telah ditemukan dan dikembangkan dengan sebegitu rumitnya dengan tujuan satu yakni untuk melindungi data. Beberapa di antaranya adalah : Cipher Substitusi, Cipher Transposisi, Vigenere Cipher, Playfair Cipher, Enigma Cipher, One Time Pad, serta Steganografi.

**Kriptografi perangkat lunak versus perangkat keras**

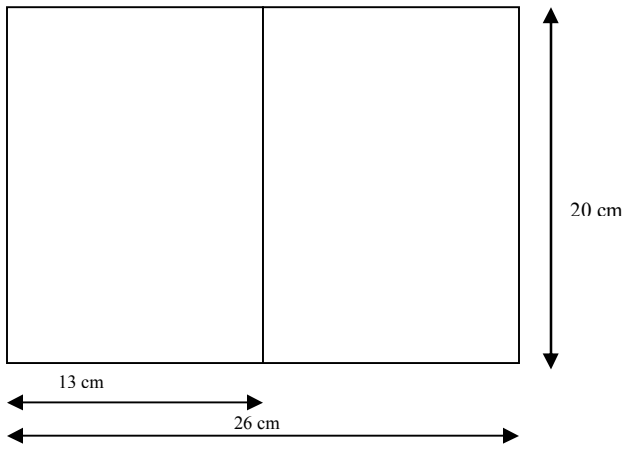
Pada publikasi oleh SafeNet mengenai evaluasi komparasi enkripsi berbasis perangkat keras dengan perangkat lunak, didapati bahwa masing-masing sebenarnya memiliki kekuatan tersendiri, namun penulisnya menyarankan bahwa enkripsi berbasis perangkat keras dalam beberapa hal lebih kuat daripada enkripsi berbasis perangkat lunak. [SAF1]

Pada makalah ini, kedua pendekatan akan digunakan, yakni enkripsi dengan pendekatan perangkat keras maupun perangkat lunak, untuk lebih memperkuat proses perlindungan data.

**Perancangan**

**Rancangan perangkat keras**

Rancangan perangkat keras akan dibentuk seukuran lembaran buku novel pada umumnya yakni : 20cm x26 cm yang dapat dilipat dua menjadi seukuran 20cm x13 cm. Dapat dilihat pada gambar 1.




**Gambar 1 Rancangan Alat**

**Rancangan Perangkat Lunak**

Perangkat Lunak yang dirancang dapat terdiri dari dua bagian yakni satu bagian bertindak sebagai sistem operasi dan satu bagian lagi bertindak sebagai perangkat lunak pembaca buku digital.

Sistem operasi yang dirancang akan bertindak seperti pengelola file, yang mendaftarkan buku digital apa saja yang terdapat di perangkat keras. Sementara itu perangkat lunak pembaca adalah perangkat lunak untuk membaca buku digital yang bertindak sebagai *decryptor*, dan pengenkrip ulang buku digital setelah selesai dibaca (buku ditutup).

**Rancangan proses Kriptografi**

Enkripsi (lihat gambar 2)

1. Buku digital dalam bentuk pdf akan dienkripsi secara perangkat lunak dengan menggunakan algoritma enkripsi simetris. (Dapat menggunakan DES, 3 DES, atau AES, RijnDael).
2. File hasil dari langkah 1 ditransfer ke perangkat keras. Pada saat proses transfer ini terjadi proses enkripsi aras perangkat keras dengan menggunakan *key* dari pemilik DigiReader.

**Dekripsi** (lihat gambar 3)

1. Proses Dekripsi hanya dilakukan saat pengguna DigiReader ingin membaca sebuah buku digital.
2. Dengan menggunakan *SmartCard* yang dimiliki oleh pemilik DigiReader ini, maka buku digital sudah dapat didekrip oleh pengguna. Namun masih dalam bentuk cipher.
3. Cipher pada hasil dekripsi langkah 1 kemudian didekrip lagi dengan menggunakan perangkat lunak pembaca yang telah dirancang. Pada tahap inilah pengguna dapat membaca isi dari buku digital tersebut.
4. Setelah pengguna mengakhiri sesi membaca, maka perangkat lunak pembaca mengenkrip lagi file tersebut.
5. Ketika pembaca mencabut *SmartCard*nya, maka semua file secara otomatis akan terenkrip di level perangkat keras.

**Rancangan pendistribusian Buku Digital**

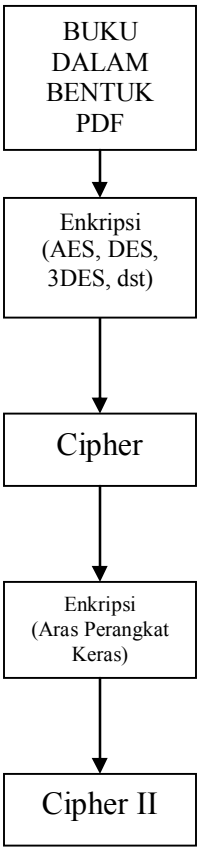
Seperti yang telah diungkapkan sebelumnya bahwa pendistribusian buku digital, meskipun telah menggunakan kriptografi berlapis, tetap juga harus menggunakan jalur pendistribusian khusus, sama seperti yang dilakukan oleh Macintosh terhadap semua karya-karya musik melalui sistem *iTunes* nya.

Setiap pemilik DigiReader yang ingin membeli buku baru harus mendatangi pusat unduh buku tertentu (layaknya sebuah toko buku) dan tidak dapat dilakukan melalui internet. Kemudian setelah menentukan buku digital mana yang akan dibeli, maka selanjutnya dilakukan proses pembayaran dan selanjutnya proses pengunduhan ke perangkat DigiReader. Dengan ini, maka tingkat perlindungan terhadap karya tulis akan semakin tinggi.

**Skema Umum**

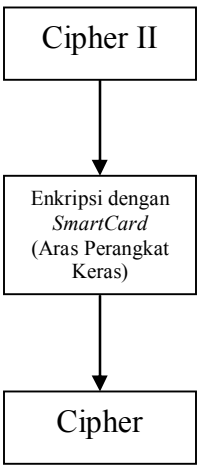
Pada bagian ini akan dirangkumkan dalam bentuk skema, mengenai skema enkripsi dan skema dekripsi pada digibook reader.

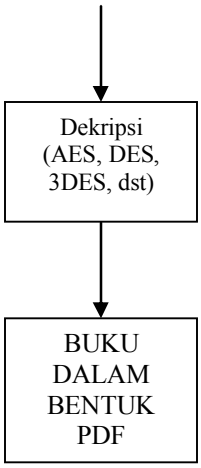
**Skema Enkripsi**




**Gambar 2 Skema Enkripsi**

**Skema Dekripsi**




**Gambar 3 Skema Dekipsi**

**Kesimpulan dan Saran**

Tantangan yang paling berat untuk mewujudkan DigiReader ini adalah dalam pembentukan perangkat keras yang bisa mengenkripsi dan mendekripsi isi media penyimpanan secara real-time, meski hal tersebut bukanlah hal yang mustahil.

Tantangan berikutnya yang timbul adalah dalam merancang perangkat keras yang nyaman yag dapat benar-benar menggantikan keberadaan sebuah buku cetak pada umumnya.

Meski terlihat bahwa hasil kriptografi dengan cara ini akan kuat seperti pada kasus iTunes, namun tetap saja akan ada cara untuk membobol perangkat DigiReader ini, namun upaya yang dilakukan memang tidak mudah.

DigiReader yang dibentuk dengan dimensi seukuran dengan buku novel pada umumnya diharapkan dapat mampu menggantikan kenyamanan yang didapat oleh pembaca sama ketika membaca sebuah buku biasa, dengan

menambahkan aspek Interaksi Manusia dan Komputer, seperti menambah fungsional membalik halaman dengan mudah, memberikan catatan kecil, mencari kata tertentu (indeks) dan sebagainya.

Dengan adanya DigiReader, diharapkan bahwa banyak orang dan banyak penerbit akan beralih dari kebiasaan membaca buku yang dicetak di atas kertas menjadi membaca buku digital melalui DigiReader ini. Hal ini diharapkan dapat berdampak signifikan kepada pengurangan penggunaan kertas sebagai bahan cetak buku, dan akhirnya berdampak pada pengurangan penebangan pohon sehingga kelestarian lingkungan dapat tetap terjaga.

## DAFTAR PUSTAKA


[MUN01] Munir, Rinaldi. Diktat Kuliah Kriptografi.

[WIK01] Application *security* - *Wikipedia*, the free encyclopedia. Tanggal Akses : 3 Maret 2010.

[WIK02] *Digital signature* - *Wikipedia, the free encyclopedia*.Tanggal Akses : 3 Maret 2010.

[ASD1] Hardware Base Disk Encryption. Dave Taylor. http: //www.askdavetaylor.com/what_is _hardware-based_disk_encryption.html Akses : 23 Maret 2010

[ID2] Facts About Paper and Paper Waste. Id2Communications.

[SAF1] Evaluating Data Encryption Solution. SafeNET.