# Analisis Keamanan Perangkat Keras Penyimpanan Data (*Data Storage Hardware*) dengan Metode Enkripsi

Eric Cahya Lesmana (13508097)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
eric_310@students.itb.ac.id

**Perkembangan dunia teknologi sangat pesat, baik dari sisi perangkat keras maupun perangkat lunak. Perkembangan ini juga seiring dengan isu keamanan pada perangkat. Salah satu hal yang perlu diperhatikan adalah keamanan untuk perangkat keras. Tujuan dari pengamanan ini adalah untuk mencegah atau membatasi penggunaan perangkat keras dari orang yang tidak berwenang. Kasus pencurian perangkat keras juga semakin banyak terjadi. Model keamanan ini juga bisa digunakan untuk mencegah pencuri untuk menggunakan perangkat sesuai dengan keinginan mereka. Dalam makalah ini dianalisis mengenai metode enkripsi pada perangkat keras penyimpan data. Pada referensi yang ada, algortima yang digunakan adalah *Triple Data Encryption Algorithm* (TDEA) Block Chiper. Algoritma ini akan dihubungkan dengan arsitektur pada perangkat keras untuk bisa dimanfaatkan untuk keamanan perangkat keras. Makalah ini hanya membahas sampai analisis dan perancangan arsitektur dari model keamanan yang diberikan, tidak sampai pada tahap implementasi.**

***Kata kunci: Triple Data Encryption Algorithm*, perangkat keras, keamanan.**

## I. PENDAHULUAN

Perkembangan teknologi sangat cepat. Setelah tahun 2000, peningkatan kualitas teknologi lebih dari dua kali lipat dibandingkan dengan tahun-tahun sebelumnya. Perkembangan ini dimulai dengan perkembangan perangkat keras yang diiringi oleh perkembangan perangkat lunak. Sampai saat perusahaan teknologi informasi, baik perusahaan perangkat lunak maupun perangkat keras, bersaing untuk selalu menjadi yang terdepan. Persaingan ini juga terjadi pada perusahaan perangkat komputer. Persaingan harga juga membuat teknologi tersebut bisa dinikmati oleh hampir seluruh lapisan masyarakat. Hal ini membuat masyarakat umum menjadi semakin mudah dalam mengiringi perkembangan tersebut.

Perkembangan teknologi dan kompetisi harga yang relatif terjangkau ini membuat kehidupan masyarakat sedikit demi sedikit bergantung pada teknologi tersebut. Penggunaan teknologi untuk mengerjakan aktivitas sehari-hari semakin melekat pada masyarakat. Komputer adalah salah satu teknologi yang tidak dapat dihindari keberadaannya. Setiap kantor memiliki komputer. Pelajar dan mahasiswa menggunakan komputer atau laptop untuk mengerjakan tugas, melakukan penelitian, atau sekedar bermain permainan.

Seiring bergantungnya kehidupan pada komputer, tindak kejahatan mulai mengalihkan targetnya ke perangkat keras ini. Banyak kasus pencurian komputer yang terjadi saat ini. Pencurian komputer ini tentu saja juga mencuri data yang ada dalam komputer tersebut. Hal ini akan sangat berbahaya ketika data yang ikut dicuri tersebut merupakan data yang bersifat rahasia, penting, dan tidak boleh diketahui orang lain. Oleh karena itu, perlu adanya metode untuk membuat data tersebut tidak bisa dibuka oleh orang yang tidak berwenang.

Kriptografi merupakan salah satu metode untuk mengamankan data. Kriptografi sudah banyak dikembangakan untuk meningkatkan keamanan suatu alat. Saat ini kriptografi bisa diaplikasikan ke dalam perangkat lunak maupun perangkat keras. Jika dihubungkan dengan kondisi sebelumnya, kriptografi bisa digunakan sebagai metode untuk meningkatkan keamanan perangkat keras. Pada makalah ini dijelaskan mengenai pemanfaatan kriptografi untuk keamanan perangkat keras, yaitu media penyimpan data. Algoritma yang digunakan adalah *Triple Data Encryption Standard* (TDES). Algoritma ini merupakan algoritma enkripsi dengan block chiper. Algoritma ini digunakan untuk mengenkripsi data pada media penyimpan data sehingga tidak bisa dibuka ketika tidak memiliki akses (kunci). Harapannya dengan metode yang diberikan bisa menambah tingkat keamanan komputer atau laptop sehingga data yang rahasia menjadi aman. Makalah ini hanya akan membahas analisis perancangan pemanfaatan algortima *Triple Data Encryption Standard* untuk media penyimpan data.

## II. DASAR TEORI

### 1. Operasi Operator Logika

Proses dalam algortima *Triple Data Encryption Standard* menggunakan operasi operator logika. Terdapat beberapa operasi operator logika, yaitu AND, OR, XOR, dan sebagainya. Operator logika yang digunakan dalam algortima *Triple Data Encryption Standard* adalah operasi XOR. Aturan umum dari operasi ini adalah

a. Jika kedua masukan nilainya sama, keluarannya adalah 0.

b. Jika kedua masukan nilainya berbeda, keluarannya adalah 1.

Untuk lebih jelasnya dapat dilihat pada tabel 2.1

Tabel 2.1 Opeartor XOR

| A | B | A XOR B |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Operasi ini akan digunakan untuk mengolah data berupa bit 0 atau 1 yang terdapat pada blok data [3].

### 2. Triple Data Encryption Standard (TDES)

*Triple Data Encryption Standard* atau dapat juga disebut *Triple Data Encryption Algorithm* merupakan algoritma yang dikembangkan dari *Data Encryption Standard*. Untuk mengenal *Triple Data Encryption Standard* perlu dijelaskan mengenai konsep dari *Data Encryption Standard*. Konsep enkripsi dari *Data Encryption Standard* adalah sebagai berikut:

a. Data yang dienkripsi merupakan blok data, selanjutnya disebut sebagai blok plainteks. Ukuran dari blok plainteks adalah 64-bit

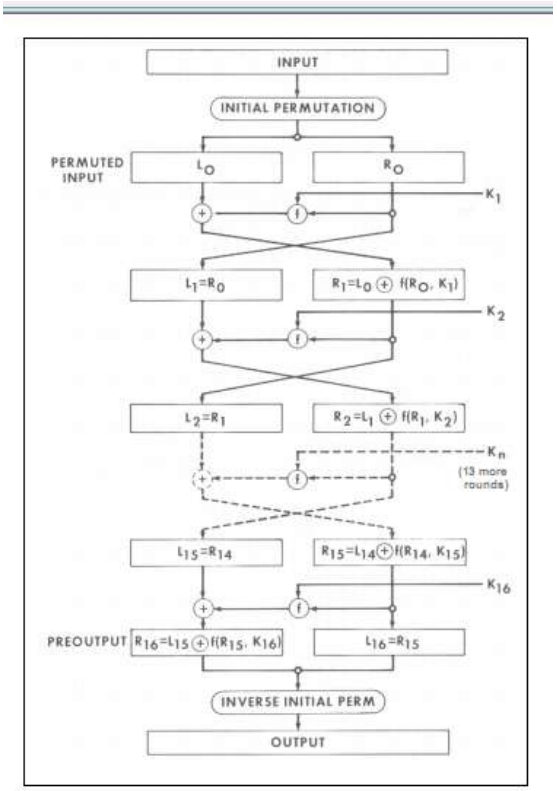
b. Blok plainteks dipermutasi dengan matriks inisial yang telah ditentukan sebelumnya.

c. Hasil permutasi tersebut dibagi menjadi dua buah bagian, yaitu: kiri (L) dan kanan (R). masing-masing panjangnya 32-bit. Bagian tersebut dimodelkan dengan model jaringan Feistel yang dinyatakan sebagai berikut:

d. Bagian kanan (R) tersebut diekspansi panjangnya menjadi 48-bit dan di-enchipering sebanyak 16 kali putaran dengan menggunakan kunci internal yang berbeda. Proses ini menggunakan operasi XOR yang melibatkan bit-bit pada bagian tersebut. Hasil dari operasi ini dikelompokkan menjadi 8 bagian, masing-masing 6-bit. Kemudian tiap bagian direduksi menjadi 4-bit dan digabung sehingga menjadi 32-bit.

e. Setelah selesai dilakukan 16 kali putaran, hasil L dan R digabungkan. Hasilnya dipermutasi dengan inversi permutasi inisial. Hasil ini merupakan chiperteks [3].

Ilustrasi dari proses tersebut dapat dilihat pada gambar 2.1




Gambar 2.1 Algoritma DES [1]

Untuk proses dekripsi merupakan kebalikan dari proses enkripsi tersebut. Proses dimulai dari permutasi dengan matriks inisial. Kemudian membagi menjadi dua buah bagian kiri dan kanan. Dilakukan *dechipering* dengan urutan kunci internal terbalik dari proses *enchipering*. Selanjutnya hasilnya digabungkan dan dipermutasi dengan invers matriks inisial [3].

Algoritma *Triple Data Encryption Standard* merupakan pengembangan dari algoritma *Data Encryption Standard*. Pada algoritma *Triple Data Encryption Standard* menggunakan tiga kali proses enkripsi dengan implementasi algoritma *Data Encryption Standard* sebanyak tiga kali. Kunci pada *Triple Data Encryption Standard* berukuran tiga kali lebih panjang dari *Data Encryption Standar*, yaitu 168-bit.

Bentuk umum TDES (mode EEE):

Enkripsi: C = EK3(EK2(EK1 (P)))

Dekripsi: P = DK1(DK2 (DK3 (C))) [4]

Proses pemilihan kunci algoritma *Triple Data Encryption Standard* ada dua, yaitu:

a. K1, K2, dan K3 adalah kunci yang saling bebas
b. K1 dan K2 adalah kunci yang saling bebas, sedangkan K1=K3.

Keamanan pada algoritma *Triple Data Encryption Standard* lebih kuat daripada . Algoritma ini dibuat dengan tujuan untuk mencegah *meet-in-the-middle attack*. Dengan panjang kunci 168-bit, terdapat $2^{168}$ kemungkinan kunci sehingga waktu pemrosesan menjadi sangat lama. Jika untuk memecahkan algoritma Data Encryption Standard memerlukan waktu ratusan tahun, pemecahan kunci ini memerlukan watku yang lebih lama lagi. Jika menggunakan komputer yang aktif dalam jaringan yang luas, sumberdaya yang diperlukan akan sangat besar. Hal ini tentu membuat pertimbangan bagi pihak yang ingin mencuri datanya [4].

### 3. Model Keamanan Perangkat Keras

Salah satu tantangan pertama dalam melindungi komputer adalah melindungi kontak langsung dengan data yang tersimpan. Pada umunya, hal yang dilakukan adalah bagamaina membungkus rahasia (data) tersebut dari orang jahat. Untuk melindungi data tersebut perlu diketahui potensi serangan dan pertahanan terhadap serangan orang jahat. Kita perlu mempertimbangkan data apa saja yang ingin diambil oleh penjahat.

Potensi serangan pada perangkat keras adalah sebagai berikut:

*a. individual chips*
*b. larger modules*
c. serangan API

Strategi pertahanan pada perangkat keras adalah sebagai berikut:

a. chip
b. luar dari chip
c. modul
*d. backward*
e. perangkat lunak

Alat yang digunakan untuk keamanan komputer adalah

a. Secure Coprocessors

alat ini dapat melakukan pengecekan terhadap integritas data umum dan integritas data yang dapat diekseksi, mengatur privrasi program, dan kerahasiaan kode program.

b. Kriptografi Akselerator

Kriptografi merupakan metode yang umum digunakan terkait masalah keamanan. Akselerator kriptografi ini digunakan sebagai media dalam melakukan pemrosesan data. Kriptografi ini bisa dimanfaatkan untuk untuk proses pengiriman data dengan enkripsi data, akses data secara langsung, dan perlindungan terhadap API.

Terdapat sebuah metode penanganan keamanan dengan nama *Hardware Security Module* (HSM) yang menggunakan kriptografi sebagai alat keamanannya.

c. Extra_CPU Functionality

*1) boot time checking*

Proses ini melakukan pengecekan terhadap segala macam 'benda' yang tidak berhak ada dalam sistem pada saat *booting*.

*2) runtime checking*

Proses ini melakukan pengecekan terhadap 'benda' yang tidak berhak ada dalam sistem ketika waktu *runtime*. Pengecekan ini dilakukan secara berkala sesuai dengan pengaturan yang dilakukan.

Selain itu juga terdapat arsitektur alternatif sebagai sarana keamanan perangkat keras, yaitu:

a. mesin konvensional

Proses yang dilakukan dalam mesin ini adalah manajemen memori, instruksi hak istimewa, dan *caching.*

b. Virtualisasi

Cara ini adalah seperti membuat ilusi berupa mesin virtual berganda. Hal ini dipakai karena kompatibilitas untuk mesin lebih terjaga. Selain itu bisa mengurangi biaya keamanan [2].

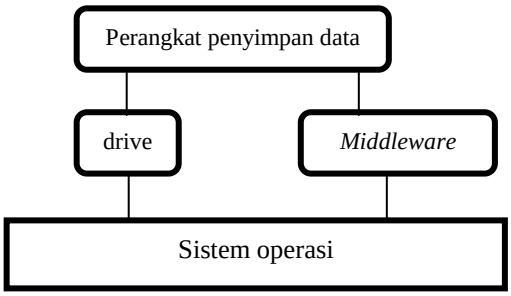
## III. ANALISIS PERANCANGAN MODEL

Pada makalah ini dianalisis cara melakukan pengamanan terhadap perangkat keras dengan algoritma *Triple Data Encryption Standard*. Hal yang perlu diperhatikan diawal adalah bentuk atau jenis serangan yang mungkin terjadi terhadap perangkat keras. Jenis serangan yang ingin dilawan adalah sebagai berikut:

a. Melakukan akses atau melihat data.
b. Melakukan penyalinan data.

c. Melakukan penghapusan data.

Dari jenis serangan tersebut bisa diselesaikan dengan metode yang dijelaskan pada dasar teori. Salah satunya adalah bisa diselesaikan dengan pertahanan di tingkat perangkat keras. Analisis model perancangan yang ingin dibangun dapat dilihat pada gambar 3.1.




Gambar 3.1 Model analisis perancangan

Model komunikasi antara perangkat lunak dengan perangkat keras adalah dengan *driver*. *Driver* merupakan *middleware* yang membuat bahasa pada perangkat keras bisa diterjemahkan dalam perangkat lunak. Jika driver tidak dapat mendeteksi perangkat keras tersebut, perangkat keras tidak dapat dibaca oleh sistem operasi. Oleh karena itu, model keamanan pada perangkat keras ini disisipkan pada *middleware* yang bisa melakukan akses terhadap *header* dari perangkat keras. Perangkat keras dalam makalah ini dikhususkan pada media penyimpanan data walaupun konsep ini dapat diaplikasikan pada perangkat keras lainnya. Konsep *middleware* yang disisipi algoritma kriptografi dijelaskan sebagai berikut:

a. media penyimpan data dikenali oleh sistem operasi melalui driver. Driver dapat mengakses informasi perangkat melalui *header*-nya. Oleh karena itu, terdapat *middleware* yang bisa 'merusak' informasi *header* tersebut.

b. *Middleware* tersebut berupa perangkat lunak yang bisa melakukan akses ke dalam sistem perangkat keras. *Middleware* ini akan melakukan enkripsi ketika media selesai digunakan dan akan melakukan dekripsi ketika media ingin digunakan.

c. Jika *middleware* tidak diaktifkan, sistem operasi dapat mengenali perangkat tersebut sehingga dapat digunakan.

Alur kerja proses enkripsi dari rancangan ini adalah sebagai berikut:

a. Perangkat keras sudah dalam kondisi dapat digunakan dalam sistem operasi.

b. *Middleware* dipasang pada sistem operasi.

c. Setelah proses pemasangan selesai, *middleware* dibuka dan dipilih perangkat penyimpan data yang ingin dienkripsi *header*-nya. Selanjutnya ditentukan mode kunci yang ingin digunakan, yaitu: berbeda semua atau kunci pertama dan ketiga sama. Kemudian kunci diisi.

d. Proses yang dilakukan setelahnya adalah proses enkripsi. Dalam proses enkripsi ini blok plainteks yang diambil adalah blok dari *header*. Setelah proses enkripsi selesai, hasil dari blok chiper disimpan ke dalam informasi *header*. Oleh karena itu, perangkat penyimpan data tersebut tidak dapat untuk diakses karena sistem operasi tidak dapat mengenali perangkat tersebut.

Alur kerja proses enkripsi dari rancangan ini adalah sebagai berikut:

a. *Middleware* sudah dipasang pada komputer dan perangkat yang sudah dienkripsi terpasang pada komputer.

b. *Middleware* dibuka dan dipilih perangkat yang ingin didekripsi. Kemudian diisi mode kunci serta nilai dari kunci yang digunakan. Selanjutnya dilakukan proses dekripsi. Setelah proses selesai, *middleware* menyimpan hasil blok plainteks ke dalam *header* perangkat. Oleh karena itu, sistem seharusnya bisa mendeteksi kembali perangkat tersebut. Hal ini disebabkan informasi perangkat sudah benar dan sistem memiliki *driver* yang sesuai

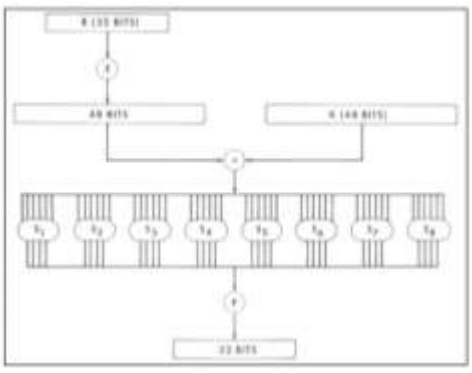
Algoritma Triple data Encryption Standard ini dipakai dalam *middleware*. Proses kerja algoritma ini secara garis besar sama dengan dasara teori yang telah dilakukan. Pada awalnya diperoleh data blok plainteks dari informasi perangkat keras. Setiap blok akan mengalami proses enkripsi. Misalnya ditentukan matrik inisialnya adalah IP. Kemudian blok tersebut dipermutasi dengan matriks tersebut. Matriks tersebut berukuran 8x8 karena ukuran blok 64-bit. Kemudian dilakukan proses *enchipering*. Proses ini diberikan kepada hasil permutasi sebelumnya yang telah dibagi menjadi dua, yaitu: kiri dan kanan. Persamaan yang digunakan adalah:

$L_n = R_{n-1}$

$R_n = L_{n-1}$ XOR $f(R_{n-1},K_n)$ ,

dengan $K_n$ adalah kunci internal setiap tahap.

Ilustrasi untuk enchipering diberikan pada gambar 3.2



Gambar 3.2 Proses enchipering satu tahap [1]

Pada proses terbut terdapat pengubahan ukuran dari 32-bit menjadi 48-bit karena disesuaikan dengan panjang kunci internal. Kemudian hasil akhirnya direduksi kembali menjadi 32-bit. Hal ini sesuai dengan penjelasan algoritma pada dasar teori. Proses tersebut dilakukan sebanyak 16 kali dengan kunci yang berbeda, sesuai dengan persamaan yang telah diberikan sebelumnya. Setelah seluruh proses selesai, hasil dari L dan R akan digabungkan. Selanjutnya hasil penggabungannya dipermutasi dengan inversi matrik inisial, yaitu $IP^{-1}$.

Blok-blok yang dienkripsi hanyalah blok informasi *header* sehingga tidak terlalu banyak dalam proses enkripsi maupun dekripsinya. Harapannya kecepatan komputasinya menjadi lebih cepat.

Hal lain yang perlu diperhatikan di sini adalah blok data tidak dienkripsi. Alasannya seperti pada penjelasan paragraf sebelumnya, yaitu untuk kecepatan komputasi. Namun tentu saja hal ini memungkinkan adanya celah keamanan dalam perancangan sistem yang diberikan.

Untuk teknisnya sendiri, perlu dirancang secara terpisah mengenai cara komunikasi *middleware* terhadap perangkat tersebut. Dalam makalah ini lebih ditekankan mengenai penggunaan algoritmanya. Dan harapannya algoritma ini bisa diterapkan melalui mekanisme yang telah diberikan sebelumnya.

## IV. PEMBAHASAN

Dari analisis perancangan yang telah dilakukan perlu dilakukan pembahasan mengenai kerja sistem, tingkat keamanan sistem, dan sisi lainnya.

Dari kerja sistem, sistem bisa melakukan enkripsi dan dekripsi. Proses ini dilakukan terpisah dengan proses penggunaan atau pengolahan data. Perangkat akan terenkripsi ketika tidak digunakan dan bisa didekripsi lagi ketika akan digunakan. Hal ini tidak mengganggu proses kerja atau penggunaan perangkat. Terkait efektifitas, sistem juga melakukan enkripsi dan dekripsi ketika diperlukan saja. Tidak harus saat *booting* atau *runtime*. Dengan kata lain, kerja sistem ini sesuai dengan kebutuhan dan tidak terlalu memberatkan sistem operasi.

Dari segi keamanan, algoritma yang digunakan merupakan algoritma yang aman. Kunci yang digunakan adalah kunci dengan panjang 168-bit sehingga ada $2^{168}$ kemungkinan kunci. Hal ini membutuhkan waktu komputasi yang sangat lama. Jika menggunakan sumberdaya yang banyak, biaya yang dikeluarkan oleh pihak yang ingin mencuri tentu sangat besar.

Seperti pada penjelasan di bagian analisis, metode ini masih memungkina adanya celah keamanan. *Middleware* ini hanya mengubah informasi *header* perangkat. Alasan kecepatan komputasi menjadi isu utama dalam supaya metode ini bisa digunakan. Hal ini memberikan dampak ketika perangkat dibuka dalam sistem operasi tertentu. Ketika pihak yan ingin mencuri langung menyalin datanya saja sangat dimungkinkan untuk membuka data tersebut di lain perangkat. Oleh karena itu, perangkat ini memerlukan sistem keamanan tambahan supaya data bisa lebih aman. Misalnya dengan enkripsi pada level data. Namun jika dibuka dengan sistem operasi, jenis serangan yang ingin dilawan bisa diatasi dengan metode ini.

Penggunaan algoritma *Triple Data Encryption Standard* ini juga cukup aplikatif diterapkan dalam perangkat keras. Model tiap blok data tidak membuat kerja sistem terlalu berat. Dan informasi dari perangkat juga disimpan ke dalam blok-blok tertentu sehingga dapat langsung digunakan.

Hal yang perlu diperhatikan lebih lanjut adalah terkait implementasi dan pengujian dari sistem ini. Teknis dari *middleware* untuk melakukan komunikasi dengan perangkat harus ditinjau secara terpisah. Dalam implementasinya tentu terdapat kesulitan yang dihadapi serta kondisi tidak ideal lainnya. Selain itu, perlu diperhatikan apakah dengan mengubah informasi *header* lebih sering dapat merusak perangkat lebih cepat. Hal ini yang semestinya diteliti lebih lanjut.

## V. SIMPULAN

Dari pembahasan dalam makalah ini dapat disimpulkan beberapa hal, yaitu:

1. Algoritma *Triple Data Encryption Standard* dapat digunakan untuk melakukan enkripsi pada perangkat keras.
2. Jenis keamanan yang dapat diatasi dengan metode yang diberikan adalah mengkases dan mengolah data pada perangkat penyimpan data melalui sistem operasi secara langsung.
3. Tingkat keamanan algoritma *Triple Data Encryption Standard* sangat kuat karena memiliki panjang kunci 168-bit. Namun masih diperlukan sistem pengamanan lainnya sebagai tambahan supaya sistem ini tetap aman ketika perangkat dibuka secara langsung.
4. Terdapat beberapa hal yang perlu diteliti lebih lanjut, yaitu mengenai implementasi sistem ini, masalah yang mungkin terjadi dalam implementasi, dan ketahanan perangkat ketika menggunakan metode ini.

## REFERENSI


[1] anonim. (2012). Diambil pada Februari 28, 2012, from http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf

[2] Commerce, U. D. (2012). Diambil pada Februari 28, 2012, from http://csrc.nist.gov/publications/nitspubs/800-12/handbook.pdf

[3] Hidayat, A. (2008). Enkripsi dan Dekripsi Data Dengan Algoritma 3DES. *Sitrotika* .

[4] Munir, R (2011). Slide kuliah IF3058 Kriptografi: Review Beberapa Algoritma Kriptografi Modern.ppt . ITB. Bandung


## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 20 Maret 2012

Eric Cahya Lesmana (13508097)