Penerapan Algoritma Kriptografi dalam Sistem *Electronic Vote*

Filman Ferdian - 13507091[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]if17091@students.if.itb.ac.id

***Abstract*—*Vote* merupakan salah satu metode untuk mengambil keputusan penting dalam kehidupan manusia. Misalnya, pemilihan keputusan suatu negara berupa kepala negara, dsb. Perkembangan teknologi telah mengenalkan kita kepada suatu sistem *electronic vote*. *Electronic vote* lebih unggul dalam hal skalabilitas, efisiensi dan akurasi. Dibalik kelebihannya, *e-vote* juga memiliki beragam permasalahan. Empat aspek yang penting diperhatikan dalam *e-vote* adalah akurasi, demokrasi, rahasia dan terbukti.**

Makalah ini membahas pada aspek kerahasiaan dalam *e-vote.* Kerahasiaan bertujuan untuk menjamin data pilihan dan pemilih tidak dapat diketahui oleh pihak manapun. Kriptografi diterapkan pada proses pengiriman data dari tempat pemilihan ke tempat tabulasi sehingga pada proses tersebut tidak dapat diketahui informasi terkait pilihan tersebut. Algoritma yang diterapkan adalah algoritma kriptografi modern yaitu DES (*Data Encryption Standard*). Algoritma ini dipilih karena dikenal secara umum dan memiliki kekuatan yang cukup baik.

***Key Words*—*Electronic vote,* kerahasiaan, DES**

I. PENDAHULUAN

Vote merupakan salah satu metode untuk mengambil Keputusan penting dalam kehidupan manusia. Dalam negara yang menganut sistem politik demokrasi, *voting* digunakan untuk mengambil keputusan negara yang sangat krusial,antara lain adalah untuk memilih wakil-wakil rakyat atau untuk memilih pemimpin negara yang baru. Perkembangan teknologi informasi saat ini telah membawa perubahan yang besar bagi manusia, termasuk cara untuk melaksanakan *voting*. Penggunaan teknologi computer pada pelaksanaan *voting* ini dikenal dengan istilah *electronic vote* atau lazim disebut dengan *e-Voting*. [1]

Electronic vote adalah penggunaan teknologi komputer pada pelaksanaan *voting*. Pilihan teknologi yang digunakan dari *e-vote* sangat bervariasi, seperti pengguna *smart card* untuk otentikasi pemilih, penggunaan internet sebagai sistem pemungutan suara, penggunaan *touch screen* sebagai kartu suara, dan masih banyak variasi teknologi lain. *E-vote* sendiri sudah digunakan di beberapa negara di benua Eropa dan Amerika. [1]

Dibalik berbagai keuntungan sistem ini bagi manusia, muncul berbagai permasalahan antara lain tingkat keamanan sistem, penggunaan internet yang rentan dengan gangguan dari luar, penggunaan perangkat lunak yang tidak dapat diaudit oleh publik. Meliza [2], dalam makalahnya, membahas tentang permasalahan keamanan dan kerahasiaan dalam sistem *e-Vote*. Pada makalah tersebut, penulis mengusulkan penggunaan *Paillier Cryprosystem* dan *Dining Cryptographers Protocol.*

Kriptografi merupakan suatu ilmu yang sudah banyak digunakan hampir di segala bidang yang terkait dengan penggunaan jaringan komputer. Bahkan kehidupan kita saat ini dilingkupi oleh kriptografi, mulai dari transaksi mesin di ATM, bank, kartu kredit, percakapan di telepon genggam, mengakses internet, dan banyak lagi. Begitu pentingnya kriptografi untuk keamanan informasi sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka orang tidak bisa memisahkannya dengan kriptografi. [3]

Kriptografi telah banyak mengalami perkembangan, terdapat berbagai macam metode yang dapat digunakan untuk memecahkan permasalahan tertentu. Umumnya, kriptografi berperan dalam menjamin kerahasiaan data. Pada makalah ini akan dibahas terkait salah satu algoritma yang dapat digunakan untuk menjamin suatu aspek keamanan pada suatu *electronic vote*.

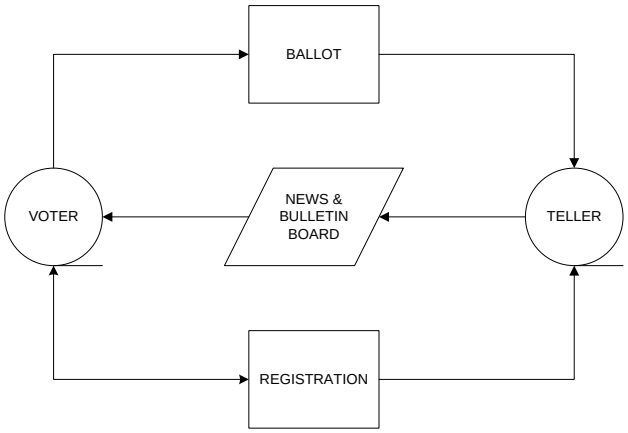
Cranor menyatakan aspek yang penting diamankan dalam suatu sistem *e-vote* adalah akurasi, demokrasi, rahasia dan terbukti. Ditilik dari aspek yang ada, permasalahan terkait kerahasiaan merupakan isu yang membutuhkan peran kriptografi. Permasalahan kerahasian tersebut harus dapat menjamin bahwa tidak ada pihak berwenang ataupun pihak lainnya yang dapat memastikan siapa pemilih dari suatu surat suara dan tidak ada pemilih yang dapat membuktikan bahwa dia sudah memilih suatu kandidat tertentu.

Berdasarkan hal tersebut, makalah ini membahas tentang proses pengiriman data pemilihan untuk menjamin kerahasiaan pemilih tersebut dengan pemanfaatan algoritma kriptografi. Algoritma yang digunakan adalah DES yang merupakan algoritma *block cipher*. Algoritma ini sudah dikenal umum dan memiliki

kekuatan yang cukup baik.

II. *ELECTRONIC VOTE*

Electronic vote adalah penggunaan teknologi komputer pada pelaksanaan *voting*. Pilihan teknologi yang digunakan dari *e-vote* sangat bervariasi, seperti pengguna *smart card* untuk otentikasi pemilih, penggunaan internet sebagai sistem pemungutan suara, penggunaan *touch screen* sebagai kartu suara, dan masih banyak variasi teknologi. Suatu dinamika aliran pada suatu *electronic vote* dapat dijabarkan sebagai berikut:



Gambar 1 Skema umum dinamika *vote*

Pada diagram dapat dijelaskan bahwa pada suatu sistem *electronic vote* data terkait *voter* dan *vote* dipisahkan. Data *voter* diproses oleh proses registrasi, sedangkan *vote* diproses melalui *ballot*.

Dalam perkembangannya, *electronic vote* masih memiliki banyak permasalahan. Laporan hasil penelitian California (2006): ditemukan bahwa tombol kuning pada Sequoia, suatu mesin *e-voting* yang mengizinkan satu orang memilih lebih dari satu kali. Venezuela (2006): Isu Hugo Chavez, Presiden Venezuela, memiliki hubungan dengan Sequoia dan kepemilikan atas *Smartmatic*, perusahaan mesin *e-voting* yang digunakan saat pemilihan umum presiden Venezuela. Ditemukan pula magnet dan PDA dapat digunakan untuk mengubah suara pada mesin *voting* layar sentuh. Ohio (2007): ditemukan permasalahan yang dapat mengancam integritas suara pada pemilu 2008. Sistem e-*voting* di Ohio, yang berbasiskan komputer, tidak sesuai dengan standard keamanan komputer yang ada dan mudah di sadap. Hal ini mengancam integritas proses pemilihan.

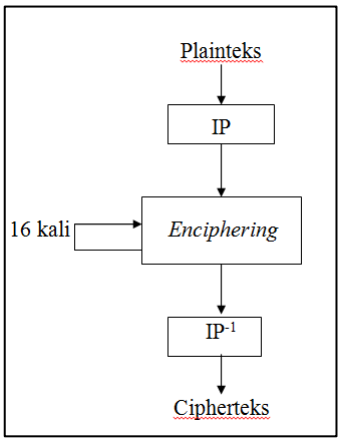
Kenyataan yang ada di lapangan tidak sesuai dengan properti yang seharusnya dimiliki oleh *electronic vote*. Para peneliti di bidang *electronic vote* menyepakati empat properti yang harus dimiliki oleh sistem *electronic vote* [4]. Pertama adalah **akurasi**. Suatu sistem *electronic vote* dikatakan akurat apabila suara tidak berubah dari suara asal, suara sah tidak dieliminasi dari perhitungan akhir, dan suara tidak sah tidak masuk dalam perhitungan akhir. Kedua adalah **demokrasi**. Suatu sistem *electronic vote* dikatakan demokrasi apabila hanya yang memenuhi syarat menjadi pemilih yang dapat memilih dan menjamin pemilih hanya dapat memilih satu kali. Ketiga adalah **rahasia**. Suatu sistem *electronic vote* dikatakan rahasia apabila tidak ada pihak berwenang ataupun pihak lainnya yang dapat memastikan siapa pemilih dari suatu surat suara dan tidak ada pemilih yang dapat membuktikan bahwa dia sudah memilih suatu kandidat tertentu. Faktor kerahasiaan yang kedua dinilai penting untuk mencegah pembelian suara. Pemilih dapat menjual suara mereka jika mampu membuktikan kepada pembeli suara.Keempat adalah **terbukti**. Suatu sistem *electronic vote* dikatakan terbukti apabila tiap orang dapat membuktikan bahwa semua suara telah dihitung dengan benar.

III. ALGORITMA KRIPTOGRAFI DES

Algoritma DES dikembangkan di IBM dibawah kepemimpinan W.L. Tuchman pada tahun 1972. Algoritma ini didasarkan pada algoritma LUCIFER yang dibuat oleh Horst Feistel. Algoritma ini telah disetujui oleh National Bureau of Standard (NBS) setelah penilaian kekuatannya oleh National Security Agency (NSA) Amerika Serikat.

DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (internal key) atau upa-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit. Skema global dari algoritma DES adalah sebagai berikut (lihat Gambar 2):

1. Blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation atau IP).
2. Hasil permutasi awal kemudian di-enciphering-sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation atau IP-1) menjadi blok cipherteks.

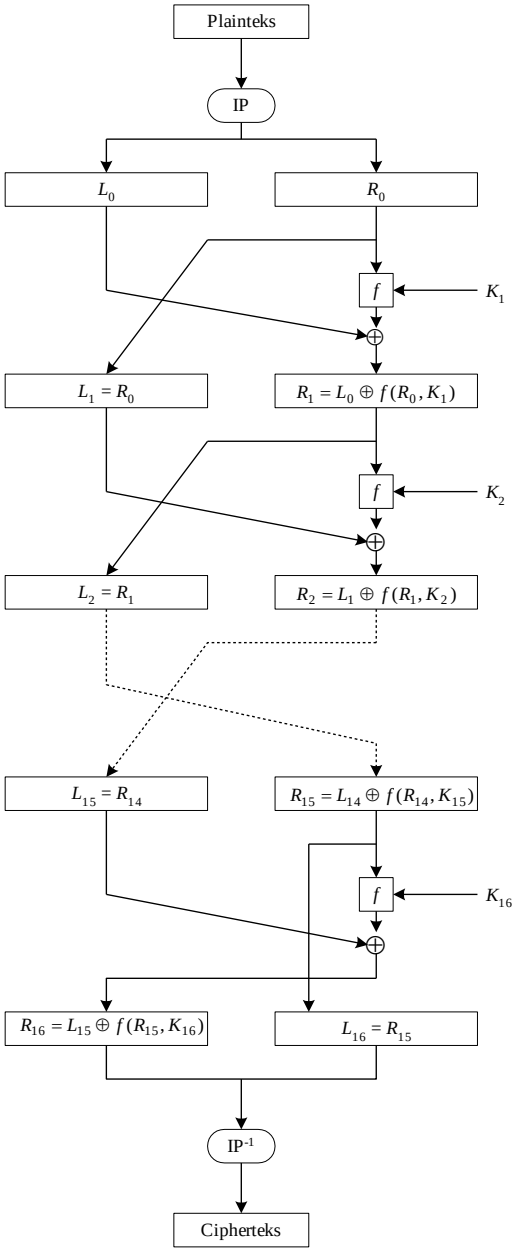


Gambar 2 Skema Algoritma DES

Di dalam proses enciphering, blok plainteks terbagi menjadi dua bagian, kiri (L) dan kanan (R), yang masing-masing panjangnya 32 bit. Kedua bagian ini masuk ke dalam 16 putaran DES. Pada setiap putaran i, blok R merupakan masukan untuk fungsi transformasi yang disebut f. Pada fungsi f, blok R dikombinasikan dengan kunci internal Ki. Keluaran dai fungsi f di-XOR-kan dengan blok L untuk mendapatkan blok R yang baru. Sedangkan blok L yang baru langsung diambil dari blok R sebelumnya. Ini adalah satu putaran DES.

Secara matematis, satu putaran DES dinyatakan sebagai

$$L_i = R_i - 1$$
$$R_i = L_i - 1 \oplus f(R_i - 1, K_i)$$



Gambar 3 Skema Rinci DES

Sebelum putaran pertama, terhadap blok plainteks dilakukan permutasi awal (initial permutation atau IP). Tujuan permutasi awal adalah mengacak plainteks sehingga urutan bit-biit di dalamnya berubah.

Karena ada 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah, yaitu K1, K2, …, K16. Kunci-kunci internal ini dapat dibangkitkan sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter. Misalkan kunci eksternal yang tersusun dari 64 bit adalah K. Dalam permutasi ini, tiap bit kedelapan (parity bit) dari delapan byte kunci diabaikan. Hasil permutasinya adalah sepanjang 56 bit, sehingga dapat dikatakan panjang kunci DES adalah 56 bit. Selanjutnya, 56 bit ini dibagi menjadi 2 bagian, kiri dan kanan, yang masing-masing panjangnya 28 bit.

Proses *enciphering* terhadap blok plainteks dilakukan setelah permutasi awal (Gambar 2). Setiap blok plainteks mengalami 16 kali putaran *enciphering* (Gambar 3). Setiap putaran *enciphering* merupakan jaringan Feistel yang secara matematis dinyatakan sebagai

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

Permutasi terakhir dilakukan setelah 16 kali putaran terhadap gabungan blok kiri dan blok kanan.

Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah K1, …, K16, maka pada proses dekripsi urutan kunci yang digunakan adalah K16, …, K1.

DES dapat dioperasikan dengan mode ECB, CBC, OFB, dan CFB. Namun karena kesederhanaannya, mode ECB lebih sering digunakan pada paket program komersil meskipun sangat rentan terhadap serangan. Mode CBC lebih kompleks daripada EBC namun memberikan tingkat keamanan yang lebih bagus daripada mode EBC. Mode CBC hanya kadang-kadang saja digunakan.

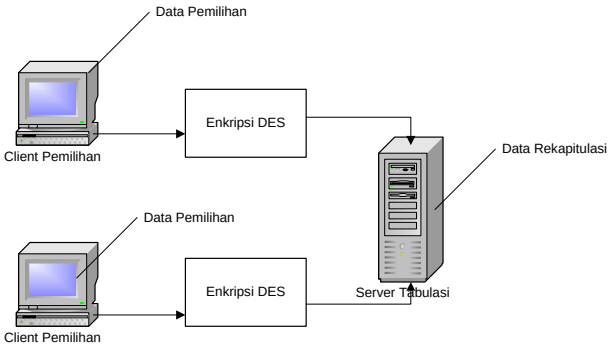
DES sudah diimplementasikan dalam bentuk perangkat keras. Dalam bentuk perangkat keras, DES diimplementasikan di dalam chip. Setiap detik chip ini dapat mengenkripsikan 16,8 juta blok (atau 1 gigabit per detik). Implementasi DES ke dalam perangkat lunak dapat melakukan enkripsi 32.000 blok per detik (pada komputer mainframe IBM 3090).

Isu-isu yang menjadi perdebatan kontroversial menyangkut keamanan DES:

1. Panjang kunci
2. Jumlah putaran
3. Kotak-S

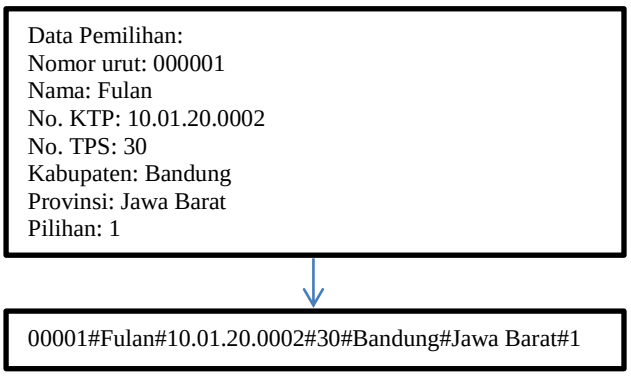
IV. PENERAPAN ALGORTIMA DES

Penerapan algoritma DES (*Data Encrypition Standard*) pada suatu sistem *e-vote* terletak pada pengiriman data dari computer klien ke computer server tempat semua data hasil pemilihan di simpan. Sesuai yang telah kita bahas sebelumnya, penerapan algoritma ini bertujuan untuk memastikan data yang dikirim tersebut tidak dapat ditelusuri pemilih dan pilihannya. Sebelum masuk ke rancangan teknis, maka kita akan membahas terlebih dahulu gambaran arsitektur dari sistem *e-vote* khususnya untuk menjamin kerahasiaan data pemilih.



Gambar 4 Arsitektur Pengamanan Data

Berdasarkan rancangan arsitektur tersebut, data yang akan ditransfer dari tempat pemilihan merupakan informasi terkait hasil pemilihan oleh pemilih dan pilihannya. Kedua jenis data tersebut harusnya tersimpan atau diolah secara terpisah. Namun, simplifikasi yang dapat diambil pada rancangan sistem ini bahwa data yang akan dikirim merupakan data pemilih yang terdiri dari misalnya: nama, nomor KTP, TPS Pemilihan, Kabupaten dan Provinsi pemilihan. Selain itu, data juga terdiri dari data pilihan. Jika coba digambarkan maka data tersebut berupa informasi sebagai berikut:



Gambar 5 Format Pengiriman Data

Pada dasarnya, format pengiriman data dapat terjadi dalam berbagai format. Format yang disampaikan pada gambar 5 dapat dijadikan sebagai bentuk dasar dari data yang akan dikirim ke server. Pada proses pengiriman sampai proses penerimaan di server, data tersebut tidak boleh diketahui oleh siapapun. Kriptografi mengambil peran dalam menyamarkan data tersebut.

Sesuai dengan konsep dari proses data pemilu, maka pengiriman data akan dilakukan minimal sebanyak dua kali atau lebih. Pengiriman pertama berfokus pada pengiriman data pemilih sebagai data orang-orang yang telah memberikan hak suara dan juga untuk mengukur validitas dari data pilihan. Sementara, pengiriman kedua adalah pengirim yang mengandung informasi pilihan. Data kedua inilah yang penting diamankan agar tidak dapat diketahui oleh siapapun asal pengirimannya.

Pada proses pengiriman data, akan terdapat kunci yang perlu digunakan untuk melakukan enkripsi maupun dekripsi. Kunci tersebut dapat diambil dari salah satu identitas yang dimiliki oleh pengguna ataupun nomor identifikasi yang diberikan oleh sistem ini. Pada pembahasan di bawah ini, kita akan mencoba melihat contoh proses enkripsi data yang ada pada gambar 5 dengan memanfaatkan kunci yang terdiri 64 bit. Pada kasus ini, kunci dapat diambil dari identifikasi nomor urut yang diberikan kepada pengguna. Ketika di tempat pemilihan kunci diambil dari nomor urut yang dihasilkan sistem ketika pemilih mendaftar. Pada tempat tabulasi kunci diambil dari nomor urut tersebut.

Cara pengiriman kunci yang dapat digunakan adalah mengirimkan sejumlah data pilihan dan sejumlah daftar kunci pada suatu TPS. Setiap data akan dicoba dengan seluruh kunci yang ada untuk menghasilkan data yang tepat yaitu data yang elemen awalnya sama dengan kunci.

Penjabaran proses enkripsi adalah sebagai berikut:

1. Data diacak dengan Initial Permutation
2. Data hasil pengacakan masuk ke tahap enciphering, yang dilakukan sebanyak 16 kali pada struktur jaringan feistle dengan pola perhitungan:
   $$L_i = R_{i-1}$$
   $$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$
3. Hasil keluaran juga akan diacak lagi dengan initial permutation sehingga menghasilkan cipherteks.

Proses dekripsi dilakukan menggunakan fungsi yang sama dengan menggunakan kebalikan dari proses enkripsi, memanfaatkan jaringan feistle. Hasil dekripsi dari sistem yang memanfaatkan kunci akan dipisah pada dua media penyimpanan, sehingga asal data sudah tidak dapat dibedakan. Proses dari algoritma DES juga masih bisa divariasi dengan menggunakan metode seperti *Electronic Code Book* (*ECB*), *Cipher Block Chaining* (*CBC*), *Cipher Feedback* (*CFB*), *Output Feedback (OFB)*. Beragam metode ini, memiliki kelebihan dan kelemahan masing-masing.

Dengan metode ini, hasil tabulasi dapat disimpulkan

tidak akan dapat menunjukkan data suatu pilihan dan data pemilihnya. Namun, dalam keberjalanannya, kita dapat melihat bahwa data yang dikirimkan dapat dienkripsi menggunakan berbagai macam algoritma. Asalkan, sistem tersebut mampu merahasiakan pemilih dan hasil pilihannya.

V. KESIMPULAN

Electronic vote memiliki empat aspek penting yang perlu diperhatikan yaitu akurasi, demokrasi, rahasia dan terbukti. Aspek kerahasiaan bertujuan untuk menjamin data pilihan dan pemilih tidak dapat diketahui oleh pihak manapun. Pemanfaatan kriptografi dalam menjamin kerahasiaan dapat dilakukan pada proses pengiriman data pemilihan dari tempat pemilihan ke tempat tabulasi. Makalah ini menerapkan algoritma DES (*Data Encryption Standard*) pada proses pengiriman data. Hasil pengiriman data dengan algoritma DES dapat dijamin terjaga.

Pada dasarnya, setiap algoritma kriptografi yang dinilai cukup kuat dapat diterapkan pada proses pengiriman data. Konsentrasi penelitian seharusnya dapat diarahkan dalam hal lain khususnya pengelolaan data pada tempat pemilihan dan tempat tabulasi. Hal ini erat kaitannya dengan cara menjamin data yang dikirim dari sisi tempat pemilihan tidak dapat diketahui pada tempat tabulasi. Namun, sistem harus dapat menjamin bahwa data pemiliha tersebut valid.

DAFTAR REFERENSI

Azhari, Rakhmad. 2005. e-*Voting*. Universitas Indonesia.

Silalahi, Meliza T. M.. 2010. Penggunaan Kriptografi pada *Electronic vote*. Institut Teknologi Bandung

Munir, Rinaldi. 2006. Kriptografi. Bandung: Informatika.

Cranor, Lorrie F. & Ron K. Cryton. 1997. Sensus : *A Security-Conscious Electronic Polling System for Internet.*

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, 23 Maret 2011

Filman Ferdian (13507091)