

# Keamanan Data pada E-KTP di Indonesia

Raymond Lukanta - 13510063

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

raymond.lukanta@students.itb.ac.id

**Abstract**—Akhir-akhir ini, di Indonesia cukup marak berita mengenai pembuatan e-KTP. Pada makalah ini, penulis akan membahas isu ini dan aspek keamanan data yang tersimpan dalam e-KTP. Untuk mengamankan data yang tersimpan, dapat menggunakan algoritma kriptografi. Kriptografi adalah teknik untuk menjaga keamanan suatu informasi. Hal yang dijaga adalah kerahasiaan data, keabsahan data, dan keutuhan data. Kriptografi dapat diterapkan pada kartu identitas elektronik untuk menjaga informasi yang terkandung dalam kartu identitas tersebut. Informasi yang terkandung dalam kartu identitas merupakan data diri dan data biometrik. Informasi-informasi tersebut diamankan dengan melakukan enkripsi secara digital. Enkripsi merupakan suatu proses yang menyebabkan informasi tersebut tidak dapat dibaca secara langsung, tapi harus dilakukan pengolahan (dekripsi). Kriptografi dapat diimplementasikan pada sebuah chip terpisah, yang dinamakan kriptoprosesor. Setelah melakukan studi pustaka, diperoleh bahwa tingkat keamanan dari e-KTP cukup tinggi, karena didukung oleh algoritma kriptografi yang sudah tepercaya.

**Index Terms**—Kriptografi, data biometrik, kartu identitas, dan kriptoprosesor.

## I. KRIPTOGRAFI

Kriptografi adalah teknik pengamanan terhadap suatu informasi. Kriptografi sudah digunakan sejak permulaan tahun 400 Sebelum Masehi oleh tentara Sparta di Yunani untuk mengirimkan pesan. Ada banyak teknik kriptografi (enkripsi) yang dapat dilakukan. Pada tahun 400 SM, teknik yang digunakan adalah dengan menggunakan alat yang disebut *scytale*. Alat tersebut terdiri dari lembaran daun papirus panjang yang dililitkan pada sebuah silinder dengan ukuran tertentu. Pada daun papirus tersebut sudah tertulis sekumpulan abjad yang tidak dapat dibaca secara langsung (*chiper text*). Abjad-abjad tersebut akan dimengerti ketika daun sudah dililitkan pada silinder. Teknik ini merupakan teknik enkripsi yang paling tua.



Gambar 1 Enkripsi pada Tahun 400SM.

Dalam kriptografi, dikenal juga beberapa istilah seperti kriptografer, kriptanalis, dan kriptologi. Kriptografer adalah orang yang membuat sebuah informasi menjadi terenkripsi. Kriptanalis adalah orang yang menganalisis *chiper text* untuk menemukan cara untuk mengembalikan *chiper text* ke teks aslinya (*plain text*). Sebenarnya, kriptanalis tidak memiliki hak untuk mengetahui teks asli, namun dengan kemampuan analisisnya, kriptanalis dapat membobol informasi tersebut. Istilah yang ketiga, kriptologi adalah ilmu yang mempelajari tentang kriptografi dan kriptanalis.

Fungsi matematis terlibat dalam melakukan proses enkripsi dan dekripsi. Kekuatan dari suatu teknik kriptografi diukur dari banyaknya usaha yang diperlukan untuk memecahkan *chiper text* menjadi teks asli. Semakin banyak usaha yang diperlukan, maka semakin banyak pula waktu yang dibutuhkan, sehingga semakin baik algoritma kriptografi yang dipakai dan semakin aman informasi tersebut.

Jika kekuatan kriptografi bergantung pada algoritma yang dipakai, maka dinamakan algoritma *restricted*. Dengan mengetahui algoritma yang dipakai, seseorang dapat dengan mudah melakukan dekripsi. Hal ini akan menjadi masalah ketika seseorang yang tadinya tergabung dalam satu kelompok memutuskan untuk keluar dari kelompok. Ketika ada yang keluar dari kelompok, maka algoritma harus diganti untuk tetap menjaga keamanan informasi yang ada di dalam kelompok.

Saat ini, kekuatan kriptografi tidak lagi didasari oleh kekuatan algoritmanya. Dengan begitu, algoritma boleh saja diketahui oleh semua orang, namun kunci untuk melakukan enkripsi atau dekripsi harus dirahasiakan. Pada teknik ini terdapat dua buah kunci, misalkan K1

dan K2. K1 adalah kunci untuk melakukan enkripsi. K2 adalah kunci untuk melakukan dekripsi. Bila  $K1 = K2$ , maka algoritma kriptografinya dinamakan algoritma simetri atau algoritma kunci pribadi (*private key*). Contoh penggunaan dari algoritma simetri adalah *Data Encryption Standard* (DES). Kelemahannya adalah pengirim dan penerima pesan harus memiliki kunci yang sama dan pengirim harus mencari cara untuk memberitahu kunci tersebut kepada penerima secara rahasia. Sebaliknya, bila  $K1 \neq K2$ , maka algoritma kriptografinya disebut algoritma asimetri atau algoritma kunci publik (*public key*). Contoh algoritma asimetri adalah RIVERS-SHAMIR-ADLEMAN (RSA).

## II. KRIPTOPROSESOR

Kriptoprosesor adalah sebuah *chip* yang di dalamnya terdapat atau berisi operasi kriptografi. Kriptografi banyak digunakan pada kartu pintar (*smart card*) seperti kartu operator telepon selular. Kriptografi menerima instruksi masukan dalam bentuk terenkripsi, setelah itu, kriptoprosesor melakukan dekripsi sehingga masukan tersebut dapat dikenali oleh program yang menjalankannya.



Gambar 2 Smart card .

## III. PEMERIKSAAN BIOMETRIK

Pemeriksaan biometrik merupakan suatu cara untuk mengenali manusia berdasarkan satu atau lebih aspek fisik dan perilaku yang dimiliki oleh manusia. Dalam Ilmu Komputer, biometrik digunakan untuk mengatur akses terhadap sesuatu. Ada dua aspek yang menjadi fokus dalam pemeriksaan biometrik, yaitu karakteristik fisik dan perilaku manusia. Aspek fisik terdiri dari sidik jari, bentuk wajah, DNA, iris, dan sebagainya. Sedangkan aspek perilaku terdiri dari ritme pengetikan,

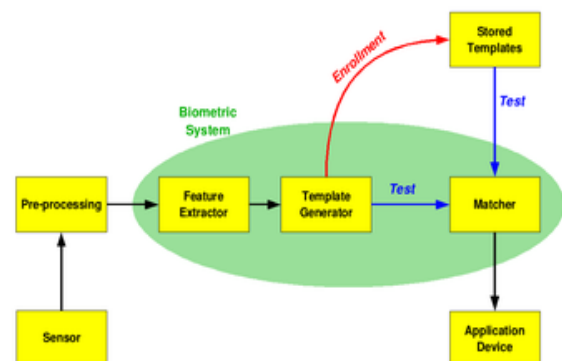
gaya berjalan, dan suara.

Pemeriksaan biometrik ini sudah diterapkan oleh negara maju pada beberapa hal, seperti pada pembuatan SIM, KTP, dan paspor. Negara-negara yang sudah menerapkan pemeriksaan biometrik antara lain Australia, Brazil, Jerman, India, Irak, Israel, Itali, Belanda, Selandia Baru, Inggris, dan Amerika Serikat. Negara kita, Indonesia sudah mulai menerapkan hal ini dalam proses pembuatan KTP, yang disebut e-KTP.

Ada tujuh faktor yang harus dipenuhi dalam menentukan objek pemeriksaan biometrik, yaitu :

1. Semua orang harus memiliki sifat tersebut.
2. Pada setiap orang yang berbeda, sifat harus berbeda.
3. Permanen : tidak berubah-ubah
4. Dapat diukur dan dianalisis
5. Performa : akurat, cepat, dan tangguh
6. Dapat diterima oleh banyak orang
7. Dapat direkayasa

Proses pertama yang dilalui oleh seseorang yang pertama kali menggunakan sistem biometrik dinamakan *enrollment*. Pada saat ini, informasi mulai diambil dari seseorang dengan menggunakan sensor, lalu disimpan di pangkalan data (*database*) atau di *chip* e-KTP. Proses ini disebut juga dengan *template generator*.



Gambar 3 Alur Proses Pemeriksaan Biometrik .

Untuk penggunaan berikutnya, tetap akan dilakukan pendeteksian terhadap aspek biometrik pemilik e-KTP. Kemudian, data yang sudah disimpan (*stored template*) akan dicocokkan dengan hasil pemeriksaan pada saat itu. Bila data cocok, maka akses akan diperbolehkan. Akan tetapi, bila data tidak cocok, maka akses akan ditolak.

## IV. E-KTP

### A. E-KTP secara Umum

E-KTP adalah dokumen kependudukan yang memuat sistem keamanan yang berbasis teknologi informasi dan bersumber pada pangkalan data kependudukan nasional. E-KTP merupakan perpaduan antara kertas dan komponen elektronik. Komponen elektronik yang dimaksud adalah *chip* yang ditanam pada kartu tersebut. *Chip* tersebut menampung data-data pribadi pemilik

kartu tersebut. Terdapat dua tipe *chip* yang bisa ditanam, yaitu *chip* yang memerlukan kontak dan *chip* yang tidak memerlukan kontak. *Chip* yang tidak memerlukan kontak mengandung minimum 32 bit EEPROM (*Electrically Erasable Programmable Read-Only Memory*). EEPROM adalah memori yang digunakan pada komputer atau peralatan elektronik lain untuk menyimpan data. Data dalam EEPROM tidak boleh terhapus walaupun daya listrik ke alat elektronik tersebut sudah dilepas.

### B. E-KTP di Indonesia

Dasar hukum pembuatan e-KTP di Indonesia adalah Undang-Undang (UU) nomor 23 tahun 2006 dan serangkaian peraturan lainnya seperti peraturan UU nomor 35 tahun 2010 yang menyatakan aturan tata cara dan implementasi teknis dari e-KTP. Menurut UU Pasal 13 No. 23 Tahun 2006 tentang Administrasi Kependudukan, nantinya e-KTP ini akan menjadi dasar dalam penerbitan paspor, Surat Ijin Mengemudi (SIM), Nomor Pokok Wajib Pajak (NPWP), Polis Asuransi, Sertifikat atas Hak Tanah, dan penerbitan dokumen identitas lainnya.

Beberapa alasan diterbitkannya e-KTP adalah karena e-KTP :

1. Tidak dapat dipalsukan
2. Tidak dapat digandakan
3. Dapat dipakai sebagai kartu suara dalam pemilu.

Data biometrik yang akan disimpan pada e-KTP adalah sidik jari dan iris mata. Sidik jari yang disimpan di pangkalan data kependudukan adalah kesepuluh jari tangan. Namun, sidik jari yang disimpan pada *chip* hanyalah jari telunjuk kiri dan jari telunjuk kanan. Kualitas sidik jari pada e-KTP lebih baik dibandingkan dengan sidik jari yang dipasang pada Surat Ijin Mengemudi saat ini; yang notabene hanya mencetak sidik jari dalam bentuk file gambar (file berformat JPEG). Sidik jari pada e-KTP akan dapat dikenali oleh *chip* yang tertanam di dalam e-KTP. Beberapa alasan dipilihnya sidik jari sebagai salah satu komponen dalam autentifikasi adalah karena :

1. Bila dibandingkan dengan komponen biometrik yang lain, sidik jari memiliki biaya paling murah.
2. Bentuk sidik jari tidak akan berubah, walaupun luka, akan kembali lagi ke bentuk semula.
3. Sidik jari setiap orang pasti berbeda, bahkan orang yang kembarpun memiliki sidik jari yang berbeda.

E-KTP yang diterbitkan terbuat dari bahan PET (*Polyethylene terephthalate*) / PETF (*Polyethylene Terephthalate Film*) / PETG (*Polyethylene Terephthalate Glycol*). Sistem pencetakan yang digunakan adalah dengan menggunakan teknologi *offset printing* dengan

*dye sublimation*. Latar belakang e-KTP dicetak dengan tinta warna. Karakteristik fisik, mempunyai ukuran 85,60 x 53,98 mm, warna biru gradasi, ketebalan dari 0,76 mm sampai dengan 1 mm kedap air (*waterproof*) berdasarkan ISO 7810:2003.



Gambar 4 Pengambilan Data Biometrik Iris Mata

### C. Struktur E-KTP

E-KTP terdiri dari beberapa lapisan, yaitu :

- Lapisan 1 :Tampak depan yang bertuliskan "KARTU TANDA PENDUDUK REPUBLIK INDONESIA". Selain itu, juga terdapat gambar Burung Garuda Pancasila dan peta kepulauan Indonesia. *Chip* ditempatkan pada sebelah kiri lapisan ini.
- Lapisan 2 : *Security printing* yang terdiri dari hologram dan *microtext* (tulisan yang hanya dapat dibaca dengan menggunakan kaca pembesar).
- Lapisan 3 : berisi PET/PETF/PETG
- Lapisan 4 : berisi *inlay pad*
- Lapisan 5 : berisi *chip*
- Lapisan 6 : berisi PET/PETF/PETG
- Lapisan 7 : berisi *inlay pad*
- Lapisan 8 : tampak belakang yang berisi *security printing* dan data diri

*Chip* yang ditanam tersebut memiliki antena yang akan memancarkan gelombang bila digesek. Gelombang yang terpancar akan dikenali oleh alat pendeteksi e-KTP sehingga alat pendeteksi tersebut akan mengetahui apakah e-KTP tersebut berada di tangan orang yang benar atau bukan.

Berikut akan dipaparkan proses pembuatan lapisan-lapisan pada e-KTP, yaitu :

1. *Hole punching* : membuat lubang pada kartu untuk tempat meletakkan *chip*.
2. *Pick and pressure* : menempatkan *chip* di kartu
3. *Implanter* : pemasangan antena (pola melingkar berulang menyerupai spiral)
4. *Printing* : pencetakan kartu
5. *Spot welding* : penekanan (*pressing*) kartu dengan menggunakan aliran listrik
6. *Laminating* : pelapisan kartu dengan plastik pengaman

Penyimpanan data di dalam *chip* sesuai dengan

standar internasional NISTIR 7123 dan Machine Readable Travel Documents ICAO 9303 serta EU Passport Specification 2006. Sedangkan bentuk KTP elektronik sesuai dengan ISO 7810.

Berikut ini adalah struktur data yang digunakan oleh *chip* :

1. Biodata yang disimpan di *chip* memiliki ukuran paling kecil 0,5 KB (Kilo Bytes)
2. Tanda tangan dengan format digital yang dikompresi dengan ukuran paling kecil 0,5 KB
3. Pas foto dengan format yang dikompresi dengan ukuran paling kecil 3 KB.

*Chip* yang digunakan pada e-KTP adalah *chip* yang nirsentuh dan berbasis mikrokontroler yang menggunakan sistem operasi terbuka. *Chip* ini memiliki *Electro Static Discharge* paling rendah ESD 2 kV. *Chip* bekerja optimal pada suhu -25°C sampai dengan 70°C. Pasokan daya (*Voltage*) yang dibutuhkan adalah dari 2,7 Volt sampai dengan 3,6 Volt.

#### D. Keamanan E-KTP

Sisi keamanan merupakan salah satu aspek penting dalam penyimpanan data secara digital. Bila masalah keamanan ini tidak ditanggulangi secara khusus, maka data-data yang bersifat pribadi dan rahasia dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Bila suatu data disimpan secara digital dan dapat diakses oleh orang lain (dicuri), maka dampak yang ditimbulkan lebih buruk bila dibandingkan dengan data analog yang dicuri. Hal tersebut karena kemudahan akses (aksesibilitas) terhadap data digital lebih mudah dilakukan dibandingkan dengan akses terhadap data analog.

Hal di atas dapat ditanggulangi dengan menerapkan sistem pengamanan terhadap data digital yang handal. Sistem keamanan yang dipakai pada *chip* adalah :

1. Pembangkit Bilangan Acak (*Random Number Generator*) berdasarkan standar AIS-31 (P2)/FIPS 140-2;
2. Mendukung autentikasi dua arah antara *smart card reader/writer* dan *chip*;
3. *Access Conditions* diterapkan per file;
4. Algoritma Keamanan (*Security Algorithm*) bersifat simetris berdasarkan algoritma: 3DES dengan panjang kunci 168 bit, AES 128 bit, atau yang setara
5. Memenuhi syarat ketunggalan transaksi (*anti tear*), *supported by chip*
6. Memiliki perangkat keras kriptoprosesor
7. e-KTP didukung dengan pengamanan melalui Sistem Manajemen Kunci (*Key Management System*).

#### E. Peralatan Pendukung

Dalam realisasinya, penggunaan e-KTP memerlukan

beberapa peralatan pendukung, antara lain alat untuk membaca dan menulis data ke *chip* dan *Automated Fingerprint Identification System* (AFIS). Di bawah ini akan dipaparkan detail dari peralatan pendukung yang diambil dari lampiran Peraturan Menteri Dalam Negeri Nomor 6 Tahun 2011[9].

Berikut ini spesifikasi dari alat pembaca dan penulis data ke *chip* :

1. Menggunakan standar ISO (International Organization for Standardization) 14443 A dan B;
2. Frekuensi dengan kisaran 13,56 MHz  $\pm$  7 KHz;
3. Kecepatan transfer data (*Baudrate*) paling rendah 100 Kilo Bit/detik;
4. Memiliki *Secure Access Module* (SAM) yang dilengkapi dengan kriptoprosesor yang sesuai dengan kebutuhan *chip*;
5. Mendukung autentikasi dua arah antara *smart card reader/writer* dan *chip*.

AFIS terdiri dari beberapa bagian, yaitu server, klien, alat pembaca sidik jari, dan aplikasi.

Server yang digunakan memiliki karakteristik sebagai berikut :

1. Platform perangkat server berbentuk *rack mounted* atau *blade*
2. Kinerja perangkat server bersifat dinamis, dapat diatur-aturl sesuai dengan kebutuhan
3. Sistem operasi berbasis *Linux/Unix/Windows* atau yang setara
4. Pangkalan Data berbasis standard RDBMS (*Relational Database Management System*), seperti *MySQL, Oracle, MS SQL Server*, atau yang setara
5. Perangkat lunak (*Software*) yang tersedia bagi AFIS Server dan AFIS Workstation
6. Kinerja perangkat lunak server dapat mendukung gugusan (*cluster*) dan dapat berskala sesuai dengan jumlah prosesor (*scalable to number of processors*).

Berikutnya, klien terdiri dari :

1. Platform perangkat keras berbasis PC
2. Sistem operasi berbasis *Linux/Unix/Windows* atau yang setara
3. Pangkalan Data berbasis standard RDBMS, seperti *MySQL, Oracle, MS SQL Server* atau yang setara
4. Perangkat lunak yang tersedia bagi AFIS PC
5. Perangkat lunak klien yang dapat mendukung verifikasi secara *realtime*.

Alat pemindai sidik jari yang digunakan memiliki spesifikasi sebagai berikut :

1. Pemindai hidup (*live scanner*) berbasis optik, pemindai satu jari (*one finger scanner*);
2. Pemindai dengan resolusi paling rendah 356 x 292 pixels dengan 500 dpi;



3. *Driver* berbasis *Linux/Windows* atau yang setara. Aspek terakhir, aplikasi yang digunakan memenuhi hal-hal di bawah ini, yaitu :

1. Fungsi dasar :
  - A. Citra Sidik Jari (*Fingerprint images*) memiliki sifat:
    - (1) 500 dpi, 256 *Gray Level*;
    - (2) *ANSI/NIST Compliant*;
    - (3) *WSQ Compression: 1:10 for tenprints, 1:15 for latent prints.*
  - B. Kode Sidik Jari mengikuti standar *ANSI/NIST ITL-1-2000, ISO/IEC 19794*
  - C. Sidik Jari tak tergantung putaran (*Rotation independent*) dan dapat diputar hingga 360 derajat;
  - D. Pemadanan (*Matching*) mendukung 1:N pemadanan dan 1:1 pemadanan yang terintegrasi
  - E. Jenis pencarian (*Type of sources*) meliputi sepuluh sidik jari-sepuluh sidik jari (*Tenprint-Tenprint*), sidik jari Laten-sepuluh sidik jari (*Latentprint-Tenprint*), dan tambahan fungsi pencarian berdasarkan dua sidik jari atau satu sidik jari;
  - F. Hasil pemadanan (*Matching Results*) ditampilkan dalam bentuk daftar ketukan (*hit list*) dengan layar terbelah (*split screen*) dan ambang batas yang dapat disesuaikan (*adjustable threshold*);
  - G. Kapasitas penyimpanan (*Storage Capacity*) bersifat tak terbatas (*Unlimited*), dapat ditingkatkan (*upgradeable*) dan kinerja dapat berskala (*scalable performance*);
  - H. Pas Photo terintegrasi secara penuh (*Fully Integrated*) atau mudah untuk interface dengan pangkalan data (*Database*) yang sudah ada dan memenuhi *JPEG color image compression*;
  - I. Biodata terintegrasi secara penuh (*Fully Integrated*) atau mudah untuk interface dengan pangkalan data (*Database*) yang sudah ada;
  - J. Apabila sidik jari tangan tidak dapat direkam, maka dilakukan perekaman kedua tangan penduduk dan *iris* yang bersangkutan ke dalam database kependudukan.
2. Performansi dari aplikasi yang digunakan dapat dinilai dari paparan di bawah ini :
  - A. Hasil pemadanan (*Matching Results*) pernah masuk dalam sepuluh besar dari *National Institute of Standards and Technology Internal Report (NISTIR)*, Amerika Serikat mulai tahun 2003 sampai dengan sekarang;
  - B. Kinerja Pemadanan (*Matching Performance*) memiliki kecepatan paling rendah 100.000

pemadanan sidik jari per detik per prosesor (core) (*fingerprint matching per second per processor (core)*), dapat berskala sesuai dengan jumlah prosesor (*scalable to number of processors*), dan memiliki kemampuan pencarian data tak terbatas (*unlimited number of data searchability*).

## V. KESIMPULAN

Upaya yang dilakukan untuk mengamankan data pada e-KTP terdiri dari dua jenjang. Jenjang yang pertama, pengamanan pada *chip* yang menggunakan pembangkit bilangan acak, autentikasi dua arah algoritma keamanan simetris 3DES dengan panjang kunci 168 *bit*, AES 128 *bit*, atau yang setara, dan terdapat kriptoprosesor. Jenjang yang kedua, sistem pengamanan juga diterapkan pada peralatan pendukung yang dipakai. Pengamanan pada jenjang kedua menggunakan kriptoprosesor pada peralatan.

Berdasarkan paparan di atas, dapat disimpulkan bahwa e-KTP memiliki tingkat keamanan yang tinggi. Akan tetapi, karena usianya yang masih muda, belum banyak pihak yang berusaha untuk membobol sistem keamanan dari e-KTP ini. Untuk itu, penelitian lebih lanjut perlu dilakukan untuk terus memperbaharui sistem keamanan yang diterapkan pada e-KTP.

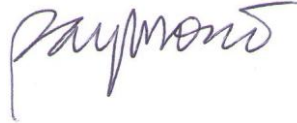
## REFERENSI

- [1] <http://id.wikipedia.org/wiki/Kriptografi>, diakses tanggal 10 Desember 2011
- [2] <http://e-ktp.com/2011/06/hello-world/>, diakses tanggal 11 Desember 2011
- [3] <http://en.wikipedia.org/wiki/Biometrics>, diakses tanggal 10 Desember 2011
- [4] [http://en.wikipedia.org/wiki/Biometric\\_passport](http://en.wikipedia.org/wiki/Biometric_passport), diakses tanggal 10 Desember 2011
- [5] [http://en.wikipedia.org/wiki/Chip\\_card](http://en.wikipedia.org/wiki/Chip_card), diakses tanggal 11 Desember 2011
- [6] <http://en.wikipedia.org/wiki/Cryptography>, diakses tanggal 10 Desember 2011
- [7] <http://en.wikipedia.org/wiki/EEPROM>, diakses tanggal 11 Desember 2011
- [8] <http://suarajakarta.com/2011/10/02/sudahkah-anda-membuat-e-ktp/>, diakses tanggal 11 Desember 2011
- [9] <http://en.wikipedia.org/wiki/Crypto-processor>, diakses tanggal 11 Desember 2011
- [10] Lampiran Peraturan Menteri Dalam Negeri Nomor 6 Tahun 2011.
- [11] Rinaldi Munir, Diktat Kuliah IF2091 Struktur Distrik, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Hal V-21 – V-25

## 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, 11 Desember 2010

A handwritten signature in blue ink that reads "Raymond". The signature is written in a cursive style with a long horizontal stroke at the end.

Raymond Lukanta - 13510063