# Pembangunan Perangkat Lunak untuk *Security* pada *Contactless Smart Card* dengan Algoritma RC4

**Stefanus Astrianto N – NIM : 13504107**

*Sekolah Tinggi Elektro dan Informatika, Institut Teknologi Bandung*
*Jl. Ganesha 10, Bandung*
E-mail : stepz007@yahoo.com

**Abstract -** Makalah ini membahas tentang perangkat lunak yang berfungsi untuk menambah aspek keamanan dalam sebuah *contactless smart card* tipe Mifare 1Kb dengan bantuan *card reader device* tipe ACR120U. Perangkat lunak ini beroperasi dengan cara mengubah konfigurasi di dalam *smart card,* serta mengenkripsi data yang akan dituliskan ke dalam kartu. Algoritma enkripsi yang digunakan adalah RC4 dan MD5 Hash.

Perangkat lunak ini ditanamkan pada sebuah komputer yang terhubung dengan *card reader device* tipe ACR120U, dengan media komunikasi USB 2.0.

Kata kunci: *smart card*, *card reader device,* enkripsi, RC4, MD5, *security*, *data confidentiality*

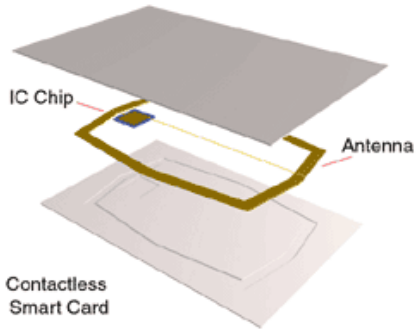
## 1. Pendahuluan

Pada saat ini penggunaan sistem informasi sangat diperlukan oleh banyak pihak. Arus informasi yang harus diolah dengan cepat dan akurat memerlukan perangkat pendukung untuk dapat mencapai tujuan yaitu pengolahan untuk mendapatkan informasi akhir secara efesien dan efektif. Sistem *smart card* merupakan perangkat yang cocok untuk diaplikasikan ke dalam suatu sistem informasi. [MAC07]

Penggunaan teknologi *smart card* sekarang ini sudah menjadi fenomena bagi masyarakat dunia. Pemakaian *smart card* pada awalnya hanya sebagai alat bantu transaksi pembayaran dan transaksi, sekarang mulai digunakan untuk keperluan lain misalnya untuk kartu parkir, passport, kartu kesehatan atau penyimpanan identitas pribadi. [MUN06]

Di dalam sebuah *smart card*, kita bisa memasukkan berbagai macam informasi. Diantaranya adalah data pribadi, data perusahaan, data transaksi, serta catatan kegiatan yang melibatkan penggunaan kartu tersebut.

Media penyimpanan pada *contactless smart card* terdiri atas sejumlah sektor, dan setiap sektor terdiri atas beberapa blok data. Untuk dapat mengakses data, pengguna harus mengetahui alamat sektor yang spesifik, kemudian *login* menggunakan kunci yang spesifik untuk setiap sektor, dimana untuk sekarang ini kunci untuk *login* ke masing-masing sektor masih *default*. [ACR06]

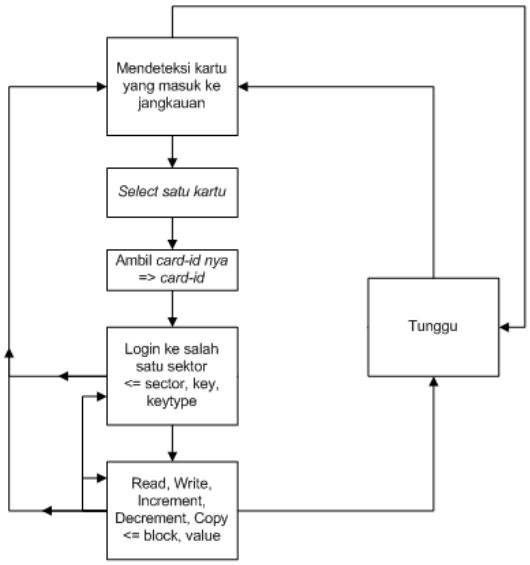



**Gambar 1 *Contactless smart card***

Salah satu komponen yang penting dalam penggunaan teknologi ini adalah aspek keamanan. Data yang tersimpan biasanya data yang bersifat rahasia yang hanya boleh diakses oleh pihak yang berhak saja. Untuk itu perlu adanya mekanisme pengamanan yang spesifik untuk melindungi informasi yang disimpan didalamnya. Sebenarnya di dalam Mifare *contactless smart card* ini sudah ada mekanisme pengamanan yang cukup baik, tetapi bentuknya masih standard, sehingga setiap pihak yang mengetahui strukturnya akan dapat menembus lapisan keamanan ini. Untuk itu perlu dibuat sebuah mekanisme pengamanan yang spesifik hanya untuk satu perusahaan saja. Bentuk *contactless smart card* dapat dilihat pada Gambar 1.

Sampai sekarang, sebagian besar perusahaan provider *contactless smart card* masih menyimpan informasi pada kartu dalam bentuk plainteks, sehingga apabila mengetahui struktur data di dalam kartu, maka akan

dengan mudah data di dalam kartu dibaca dan dimodifikasi. Untuk itu diperlukan sebuah metode pengamanan yaitu pengubahan konfigurasi, yang mengubah *password* setiap sektor menjadi unik. Tujuannya adalah supaya tidak semua orang bisa *login* ke sektor tersebut kemudian membaca dan memodifikasi isi di dalamnya. Selain itu perlu diaplikasikan juga sebuah algoritma enkripsi yang mengenkripsi blok data yang ada di dalam *smart card*. Sehingga apabila lapisan keamanan pertama yaitu *password* sektor tersebut ditembus, maka data yang terbaca masih berupa *cipherteks*. Untuk lebih jelasnya, proses baca/tulis kartu dapat dilihat pada Gambar 2.




**Gambar 2 Alur baca/tulis kartu**

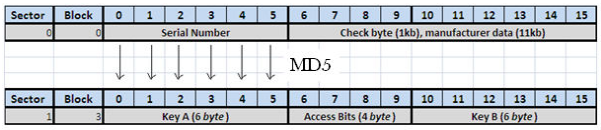
## 2. Pengubahan Konfigurasi *Smart Card*

*Mifare contactless smart card* yang berukuran 1kb mempunyai 2 macam kunci *login* untuk dapat masuk ke dalam sektor, yaitu kunci A dan kunci B. Keduanya bisa dipakai untuk mengamankan kartu, tetapi umumnya, kunci yang dipakai hanyalah kunci A saja, karena dianggap dengan menggunakan satu macam kunci saja sudah relatif aman. Pada keadaan awal, kunci untuk masuk setiap sektor pada Mifare *contactless smart card* adalah default. Secara *default*, isi kuncinya adalah :

***Key* A** : FF FF FF FF FF FF (Phillips)
***Key* B** : FF FF FF FF FF FF (Phillips)
***Access Condition* :** FF 07 80 69

Hal ini sangat rawan, karena pada kondisi ini berarti setiap *smart card programmer* pasti bisa bisa mengakses isi setiap sektor pada kartu, bahkan mengubah isinya. Sehingga untuk menangani hal ini, sebelum digunakan, setiap kartu harus diinisialisasi dan diubah kuncinya. Dalam aplikasi ini, kunci untuk masuk ke sektor diubah dengan mengambil *card-id* sebagai umpan masukannya. Pada aplikasi ini, sektor yang digunakan adalah sektor keenam saja, sehingga perubahan kunci untuk masuk sektor hanya dilakukan pada sektor keenam saja.

Cara pemakaian umpan adalah dengan mendeteksi *card-id* yang terbaca dari kartu kemudian mengambil nilai *hash*-nya. Hasil keluaran nilai hash ini adalah 32 karakter heksadesimal. Dari deretan karakter ini, diambil 6 karakter pertama, yang kemudian dipakai untuk menggantikan kunci untuk login pada sektor pertama.

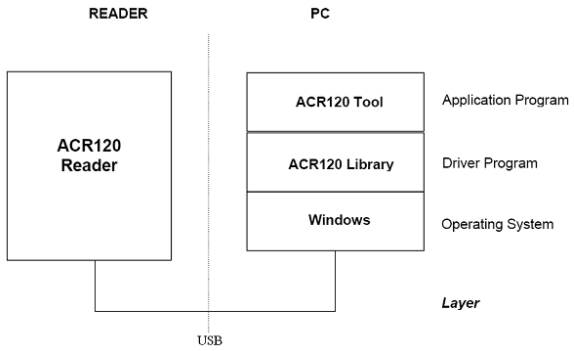



**Gambar 3 Pengubahan kunci login**

Kunci untuk masuk ke sektor terdapat pada blok terakhir dari setiap sektor, atau yang biasa disebut sebagai *sector trailer*. Pengubahan kunci *login* sektor pertama dilakukan dengan cara menimpa atau menuliskan karakter baru ke dalam 6 *byte* pertama blok ke-4 dari sektor tersebut. Hanya 6 *byte* pertama saja yang diubah, karena *byte* selanjutnya adalah *access condition* yang mengatur hak akses ke sektor tersebut. Setelah 6 *byte* tersebut diubah, maka otomatis pada proses *login* selanjutnya, harus sudah menggunakan kunci yang baru. Skema pengubahan kunci login dapat dilihat pada Gambar 3.

## 3. Enkripsi Data dalam *Smart Card*

Aplikasi yang dibuat pada tugas akhir ini akan ditanamkan pada komputer yang terhubung dengan *card reader device*. *Device* itulah yang akan digunakan untuk baca sekaligus tulis data pada *smart card*. Pada kenyataannya, *card reader* inilah yang akan berinteraksi langsung dengan *user*. Aplikasi yang dibuat ini termasuk pada ACR120 *tool*, yaitu aplikasi yang berfungsi untuk mengendalikan proses-proses yang dilakukan oleh card reader melalui *device driver*. Hubungan antara *reader* dan aplikasi dijelaskan pada Gambar 4.

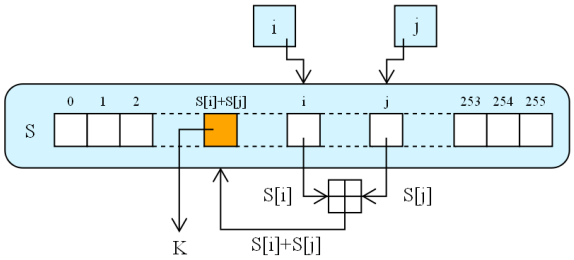



**Gambar 4 Hubungan antara reader dan aplikasi**

Salah satu hal yang menjadi masalah penting dalam proses transaksi menggunakan *smart card* adalah *processing time,* yaitu waktu yang dibutuhkan dari mulai *card reader* mendeteksi bahwa ada kartu didalam jangkauan sensornya, pembacaan, autentikasi, transaksi, sampai pemutusan hubungan antara *reader* dengan kartu. *User* pasti akan merasa lebih nyaman dan tenang apabila proses transaksi yang dilakukan itu cepat selesai. Untuk itu, maka pemrosesan transaksi pada kartu harus seefisien dan sesimpel mungkin, termasuk proses enkripsi dan dekripsinya tidak boleh terlalu signifikan menambah *processing time* nya.

Data disimpan di dalam *smart card* dalam bentuk blok-blok data yang masing-masing berisi *byte* data. Dan penyusunan di dalamnya diletakkan dalam sektor-sektor yang terpisah. Sedangkan untuk pembacaan datanya, harus melalui proses *login* terlebih dahulu ke dalam sektor yang diinginkan. Sekali *login* untuk sekali pengaksesan ke satu sektor. Setelah *login* berhasil, baru kemudian sistem dapat melaksanakan operasi baca / tulis terhadap kartu tersebut. Untuk itu, maka algoritma enkripsi yang tepat adalah RC4. Selain itu, menilik kebutuhan bahwa algoritma enkripsi itu tidak boleh terlalu rumit dan membebani *card reader,* maka harus dipilih algoritma yang cukup sederhana, tapi kuat.

Untuk melakukan enkripsi dengan menggunakan algoritma RC4, ada beberapa parameter yang dipergunakan. Yaitu blok permutasi S-Box, serta kunci U. Supaya setiap proses enkripsi memiliki proses yang unik, maka blok permutasi S itu diisi dengan suatu parameter yang unik pula, yaitu *card-id. Card-id* adalah 4 *byte* unik yang ada di sektor pertama blok pertama pada setiap Mifare *contactless smart card. Card-id* tersebut harus dimodifikasi supaya panjangnya menjadi 256 *bytes.* Caranya adalah dengan mengambil nilai *hash card-id* tersebut, kemudian mengisikannya ke blok permutasi S-Box. Fungsi *hash* yang digunakan adalah MD5. Nilai *hash* yang dihasilkan oleh fungsi MD5 berukuran 32 *byte*, sementara ukuran blok permutasi S-Box adalah 256 *byte*, untuk itu nilai *hash* yang didapat harus diisikan secara berulang sebanyak 8 kali. Hal ini dilakukan untuk menambah performa keamanannya. Karena apabila *card-id* tersebut hanya diambil mentah-mentah, maka kemungkinan tertebaknya parameter algoritma itu akan sangat mudah.




**Gambar 5 *Key Schedulling***

Setelah larik permutasi S-Box dan kunci U siap, maka dilakukan proses *key-scheduling* yang prosesnya dapat dilihat pada Gambar 5. Yaitu proses untuk membangkitkan aliran-bit-kunci. Pada saat *card reader* melakukan proses penulisan, *reader* akan langsung menuju ke sektor yang diinginkan. Login ke sektor tersebut diinisialisasi, dan bersamaan dengan proses penulisan *byte-byte*nya, maka dilakukan proses *pseudo-random generation algorithm.* Jadi pada setiap *byte*nya, terjadi 4 proses yang berjalan berurutan, yaitu men-*generate* aliran-bit-kunci, meng-XOR-kan dengan *byte* yang akan dituliskan, menuliskan *byte* yang sudah dienkripsi ke dalam *memory smart card,* kemudian mengacak ulang isi kotak permutasi S-Box. Proses ini diulangi sebanyak jumlah *byte* yang akan dituliskan.

## 4. Analisa Hasil Penambahan Aspek Keamanan

Secara garis besar, ada dua aspek keamanan yang ditambahkan oleh perangkat lunak ini. Yaitu pengubahan konfigurasi kartu dan enkripsi data. Penambahan aspek keamanan ini hanya dilakukan pada kartunya saja dengan tujuan supaya pihak yang tidak berhak tidak dapat membaca, memodifikasi dan menggunakan data di dalam kartu.

Proses modifikasi dilakukan dengan menggunakan parameter yang unik dari setiap kartu, yaitu *card-id*. Setiap kartu mempunyai *card-id* yang berbeda, sehingga setiap kartu mengalami proses pengubahan konfigurasi yang unik antara satu kartu dengan kartu yang lain. Proses ini mengurangi kemungkinan celah keamanan dari serangan *known-plaintext-attack.* Hal

ini dilakukan dengan menggunakan asumsi bahwa tidak akan pernah ada dua kartu yang mempunyai *card-id* yang sama.

Untuk keadaan standar, sistem keamanan yang dihasilkan perangkat lunak ini sudah cukup aman, dan sesuai dengan tujuan awal perancangan perangkat lunak, yaitu supaya pihak yang mempunyai *card reader* dan mengerti konfigurasi kartu tidak dapat menggunakan kartu tersebut. Tetapi perangkat lunak ini masih mempunyai celah, yaitu pada proses komunikasi antara kartu dengan *reader* yang terjadi secara *contactless*. Hal ini memungkinkan adanya proses penyadapan di antaranya. Aspek ini bisa ditangani dengan cara menginkripsi komunikasi data antara kartu dengan *reader,* tetapi hal ini membutuhkan tingkat pemrograman lebih lanjut, yaitu pemrograman pada *hardware card reader* nya.

## 5. Kesimpulan dan Saran

Kesimpulan yang dapat diambil setelah melakukan implementasi dan pengujian perangkat lunak adalah sebagai berikut :

1. Perangkat lunak dengan bantuan *card reader device* dapat mendeteksi dan menggunakan *contactless smart card,* serta memodifikasi konfigurasinya.
2. Perangkat lunak dapat menggunakan *card-id* yang unik dari setiap kartu untuk parameter modifikasi kunci dan parameter enkripsi.
3. Perangkat lunak mampu menambah aspek keamanan dalam Mifare *contactless smart card,* yaitu dengan cara mengubah kunci *login*, dan mengenkripsi data.
4. Perangkat lunak mampu membaca dan mengembalikan data yang sudah terenkripsi menjadi ke bentuk semula yang dapat dimengerti oleh pengguna.
5. Pada saat sistem mengganti kunci login, sistem pasti *error,* tapi akan kembali seperti semula saat sistem di-*restart.*
6. Perangkat lunak sudah mampu menambahkan aspek *security* pada *smart card,* tapi masih ada beberapa hal yang harus ditambahkan supaya bisa menjadi suatu sistem informasi yang baik.

Saran yang dapat diberikan untuk pengembangan perangkat lunak lebih lanjut adalah sebagai berikut :

1. Perlu diperbaiki bagaimana cara supaya pada saat penggantian kunci *login,* sistem tidak *error*
2. Untuk desain perangkat lunak yang akan digunakan pada transaksi sebenarnya, perlu menggunakan metode pengacakan yang lebih unik, misalnya pada peletakan pada blok data, bisa diletakkan pada *byte-byte* dengan urutan acak.
3. Dalam menuliskan suatu nominal ke kartu, sebaiknya dilakukan dengan metode yang lebih aman. Misalnya dengan mengurangkan suatu nominal yang sangat besar (cth : 10.000.000) dengan nominal sebenarnya, baru kemudian menuliskan hasilnya.
4. Untuk melindungi perangkat lunak ini dari penggunaan oleh pihak-pihak yang tidak berhak, sebaiknya diberi pengaman tambahan, yaitu autentikasi pengguna.
5. Untuk diterapkan dalam sebuah system informasi, sebaiknya perangkat lunak juga melakukan suatu pencatatan di *database,* hal ini diperlukan untuk menghindari modifikasi kartu oleh pihak selain perusahaan pemilik kartu
6. Perlu dipikirkan kembali bagaimana cara memanajemen kunci enkripsi supaya lebih aman
7. Karena MD5 merupakan algoritma yang sudah banyak dikenal, maka sebaiknya *string* yang akan digunakan untuk mengganti kunci sektor dienkripsi sekali lagi.

## 6. Daftar Pustaka


[IDW08] http://www.idwholesaler.com/resources/technology.htm, diakses 18 Oktober 2008 06.07 WIB

[WIK08] http://en.wikipedia.org/wiki/Image:RC4.svg, diakses 11 November 2008 10.07 WIB

[MUN06] Munir, Rinaldi. Kriptografi. Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung. 2006.

[ACR06] Advance Card System Ltd. ACR120S Contactless Reader / Writer Communication Protocol, Advance Card System Ltd. 2006.

[MIF102] Philips Semicondutor. Mifare Standard 1 kByte Card IC MF1 IC S50

Functional Specification, Philips. 2006.
[MIF402] Philips Semicondutor. Mifare Standard 4 kByte Card IC MF1 IC S70 Functional Specification, Philips. 2006.
[MAC07] PT Mulia Agung Cempaka. Smart Card System untuk Universitas Bina Nusantara, MAC. 2007.
[MD508] http://www.frez.co.uk/freecode.htm#md5, diakses pada tanggal 1 Mei 2008, pukul 10.00