UNIVERSITAS INDONESIA

RANCANG BANGUN SIMULASI AUTENTIKASI GSM DENGAN ALGORITMA A3 MENGGUNAKAN MIKROKONTROLLER AT89S52

TUGAS AKHIR

T.MAULANA HABIBI
06 06 04 292 2

FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
DEPOK
DESEMBER 2008

UNIVERSITAS INDONESIA

RANCANG BANGUN SIMULASI AUTENTIKASI GSM DENGAN ALGORITMA A3 MENGGUNAKAN MIKROKONTROLLER AT89S52

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana teknik

T.MAULANA HABIBI
06 06 04 292 2

FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
DEPOK
DESEMBER 2008

HALAMAN PERNYATAAN ORISINALITAS

Tugas akhir ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama : T. MAULANA HABIBI

NPM : 06 06 04 292 2

Tanda Tangan : ……

Tanggal : 30 Desember 2008

HALAMAN PENGESAHAN

Tugas akhir ini diajukan oleh :

Nama	: T.Maulana Habibi
NPM	: 06 06 04 292 2
Program Studi	: Teknik Elektro
Judul Tugas akhir	: **RANCANG BANGUN SIMULASI AUTENTIKASI GSM DENGAN ALGORITMA A3 MENGGUNAKAN MIKROKONTROLLER *AT89S52***

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro Fakultas Teknik, Universitas Indonesia

DEWAN PENGUJI

Pembimbing	: Fitri Yuli Zulkifli, ST, M.Sc	
	NIP. 132 206 671	(……)
Penguji	: Dr. Ir. Arman D. Diponegoro, M.Eng	
	NIP. 131 476 472	(……)
Penguji	: Arief Udhiarto, ST. MT	
	NIP 040 050 003	(….....)

Ditetapkan di : Ruang Multimedia A LT.2 DTE Universitas Indonesia Depok

Hari / Tanggal : Senin, 22 Desember 2008

UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kepada **ALLAH S.W.T**, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan tugas akhir ini. Penulisan tugas akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Jurusan Elektro pada Fakultas Teknik Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan tugas akhir ini, sangatlah sulit bagi saya untuk menyelesaikan tugas akhir ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

(1) Fitri Yuli Zulkifli, ST M.Sc, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan tugas akhir ini;

(2) DR.Ir Arman Djohan Diponegoro, M.Eng selaku dosen pembimbing teknis telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan tugas akhir ini;

(3) Arief Udhiarto, ST. MT terima kasih atas pengertian dan kritikannya,

(4) Orang tua dan keluarga saya yang telah memberikan bantuan dukungan material dan moral; dan

(5) Teman-teman dekatku di kampus teknik elektro, Pak Herli, Zaenal, Ingot, Permadi, Yuskar fisip_crime dan teman-temanku yang tidak dapat saya sebutkan satu-persatu yang telah membantuku baik secara langsung maupun tidak langsung, terima kasih semua atas bantuannya.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga tugas akhir ini membawa manfaat bagi pengembangan ilmu.

Depok, 30 Desember 2008

Penulis

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : T.Maulana Habibi
NPM : 0606042922
Program Studi : Teknik Elektro
Departemen : Teknik Elektro
Fakultas : Teknik
Jenis karya : Tugas Akhir

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

RANCANG BANGUN SIMULASI AUTENTIKASI GSM DENGAN ALGORITMA A3 MENGGUNAKAN MIKROKONTROLLER AT89S52

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 30 Desember 2008

Yang menyatakan

(T.Maulana Habibi)

ABSTRAK

Nama : T. Maulana Habibi
Program Studi : Teknik Elektro
Judul : **RANCANG BANGUN SIMULASI AUTENTIKASI GSM DENGAN ALGORITMA A3 MENGGUNAKAN MIKROKONTROLLER AT89S52**

Perkembangan telepon selular setiap tahun semakin meningkat, baik dari segi kuantitas yaitu pertambahan jumlah pengguna maupun segi kualitas yaitu peningkatan fitur yang disediakan oleh operator. Di lain sisi berdasarkan hasil penelitian pada tahun 2003 menunjukkan 850 juta telepon selular mengalami penyadapan *(eavesdro*p) pada saat terjadi panggilan. Untuk menjamin aspek keamanan, sistem jaringan GSM *(Global System for Mobil*e) menawarkan tiga macam keamanan, salah satunya yaitu autentikasi. Kebutuhan autentikasi dilakukan dengan penggunaan *smart card* yang lebih dikenal dengan nama *SIM car*d.

Autentikasi merupakan prosedur yang digunakan untuk memeriksa keabsahan identitas pelanggan GSM yang mengakses jaringan GSM dan akan menggunakan semua fasilitas layanan (*features*) yang ditawarkan oleh jaringan GSM.

Autentikasi GSM dilakukan menggunakan algoritma tertentu yaitu algoritma A3, Algoritma A3 adalah algoritma autentikasi dalam keamanan GSM yang berfungsi untuk membangkitkan response yang lebih dikenal dengan Sres sebagai jawaban dari *random challenge* yang dikenal dengan RAND.

Tugas Akhir ini berupa rancang bangun simulasi yang mensimulasikan proses autentikasi GSM khususnya pada sisi pelanggan dengan cara mensimulasikan triplet-triplet autentikasi sehingga menghasilkan nilai Sres (*Signal Response*) sebesar 32 bit sesuai dengan spesifikasi ETSI (*European Telecommunication Standarts Institute*), dengan menggunakan alat bantu simulasi Mikrokontroller AT89S52.

Tugas Akhir ini berhasil mensimulasikan proses autentikasi GSM dengan algoritma A3 dengan memanfaatkan kemampuan mikrokontroller AT 89S52 sebagai komputasi data dari triplet-triplet autentikasi GSM, yang ditampilkan dalam penampil LCD (*Liquid Crystal Display*) dan Hyper terminal.

Kata Kunci :

Autentikasi GSM, Algoritma A3, Mikrokontroller

ABSTRACT

Name : T.Maulana Habibi
Study Program *: Electrical Engineering*

Title ***: DESIGN AND CONSTRUCTIONS OF GSM AUTHENTICATION BY ALGORITMA A3 USING MICROCONTROLLER AT89S52***

A Cellular communication technology has been improved recently, not only in quantity aspect where the amount of user growth increased rapidly, but also in quality aspect which indicated by the ability of operator /vendor providing many new features. In the other side, Security issues became more and more concerned. Based on a research held in 2003, more than 850 million cellular communication users had been tapped (eavesdrop) during their call session. For security issues, the GSM network (Global System for Mobile) offered three kind of security system. One of its security systems is authentication system. This authentication system is implemented by the use of smart card which more popular known as SIM card system.

Authentication is a procedure which is used to check validity identity of GSM subscribers which access GSM network and use all of the facility offered by GSM networks.

GSM Authentication is done to use certain algorithm; The Algorithm A3 is authentication algorithm in security and safety of GSM functioning to generate response which is known well with Sres as answer from random challenge recognized as Rand.

This final project is to design and construct the simulation and process of GSM authentication appropriate with mobile station, the construct uses triplet's authentication to generate Sres (Signal Response) using Microcontroller AT 89S52
This final project successfully simulate, the process of GSM Authentication with Algorithm A3 using capability of microcontroller AT 89S52 as computation data processor, displayed by LCD (Liquid Crystal Display) and HyperTerminal

K*eyword:*
Authentication, Algorithm A3, Microcontroller

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

GSM	Global System for Mobile communication
MS	Mobile Station
A3	Algorithm Function for Authentication
Ki	Individual Subscriber Authentication Key
Rand	Random Number
SRes	Signal Response
SIM	Subscriber Identity Module
BTS	Base Transceiver Station
MSC	Mobile Service Switching Centre
VLR	Visitors Locations Register
AuC	Authentication Center
ISDN	Integrated Service Digital Network
BSS	Base Station Sub-system
BSC	Base Station Controller
NSS	Network and Switching Sub-system
EIR	Equipment Identity Register
HLR	Home Location Register
EIR	Equipment Identity Register
PSTN	Public Switched Telephone network
PIN	Personal Identification Number
PUK	Personal Unblocking Key
IMSI	International mobile sub-scribers identity
PPI	Programmable Peripheral Interface

BAB 1
PENDAHULUAN

1. 1 LATAR BELAKANG

Perangkat dan aplikasi telepon bergerak sering tidak dapat dipisahkan lagi dari dalam kehidupan manusia saat ini. Penggunaan perangkat dan aplikasi telepon bergerak saat ini sangat luas di dalam berbagai macam bidang kehidupan. Bahkan banyak kegiatan penting dilakukan hanya dengan menggunakan perangkat dan aplikasi telepon bergerak.

Karakteristik perangkat telepon bergerak tergabung dalam jaringan dengan menggunakan gelombang radio mengakibatkan setiap data yang dikirimkannya dapat diambil oleh pihak yang tidak berkepentingan [1]. Karakteristik ini mendorong munculnya suatu metode pengamanan setiap pihak yang terlibat dalam penggunaan perangkat dan aplikasi telepon bergerak.

Keamanan informasi dari berbagai macam ganguan merupakan persoalan utama baik pada jaringan kabel atau nirkabel. Keamanan sistem informasi mencakup keamanan jaringan, keamanan informasi dan fisik/peralatannya itu sendiri. Sistem keamanan dibuat untuk mengatasi masalah autentikasi, integritas informasi dan masalah pengenalan. *Mobile phone/Hand phone* (HP) yang memberikan kemudahan dalam berkomunikasi dengan siapa saja dan dimana saja, telah menjadi bagian yang penting dalam proses bisnis dan kehidupan masyarakat. Persoalan utamanya adalah informasinya saat ini mudah disadap, karena menggunakan sinyal radio sebagai saluran transmisinya, walaupun telah banyak mengeluarkan biaya yang sangat besar dalam penanggulangannya. Diperlukan suatu langkah–langkah pengamanan diantaranya dapat berupa autentikasi simcard GSM.

Adanya beberapa kelemahan pada sistem keamanan pada komunikasi telepon bergerak di area keamanan autentikasi pengguna terutama mudahnya dilakukan pengkloningan terhadap pesawat telepon merupakan latar belakang dari rancang bangun simulasi ini.

Pada dasarnya ada tiga area keamanan yang ditawarkan oleh GSM, yaitu:

1. Autentikasi pengguna
2. Kerahasian data dan sinyal
3. Kerahasian pengguna

Pada tugas akhir ini pembahasan rancang bangun menitik beratkan di segi keamanan autentikasi pengguna, dimana Autentikasi pengguna dibutuhkan untuk mencegah pengguna yang tidak berhak memasuki jaringan dan mengklaim bahwa pengguna yang tidak berhak tersebut adalah subscriber. Jika hal ini terjadi, maka dengan mudahnya ada kemungkinan untuk membajak *account* seseorang dan seolah-olah pengguna yang tidak berhak tersebut adalah *account* tersebut. Autentikasi pengguna dilakukan agar hanya pengguna yang terdaftar dan berhak saja yang dapat menggunakan layanan operator jaringan. Selain itu digunakan agar tagihan dikenakan pada pengguna yang tepat, yang memang memanfaatkan layanan jaringan. Keamanan algoritma ini tergantung pada kunci rahasia user Ki yang beririsan antara *mobile phone* dan jaringan GSM. Panjang kunci yang biasa digunakan oleh operator adalah 128 bit.

Keamanan dari kesuluruhan sisitem keamanan GSM terletak pada kunci rahasia, Ki. Jika kunci ini berhasil diperoleh maka seluruh informasi lain mengenai pelanggan yang bersangkutan dapat diperoleh. Sewaktu penyerang mampu untuk mengambil kunci Ki, maka pengguna yang tidak berhak tidak hanya mampu mendengarkan panggilan telepon pelanggan, tetapi juga menggunakan panggilan dengan menggunakan nomor pelanggan asli, karena pelanggan yang tidak berhak dapat menirukan legitimasi pelanggan. Jaringan GSM memiliki gelombang penjegal untuk jenis serangan seperti ini, mekanismenya yaitu dua telepon dengan ID yang sama dijalankan secara bersamaan, dan jaringan GSM mendeteksinya ada telepon yang ’sama’ pada lokasi yang berbeda, maka secara otomatis jaringan GSM akan menutup *account* tersebut, untuk mencegah penyerang melakukan pengkloningan telepon.

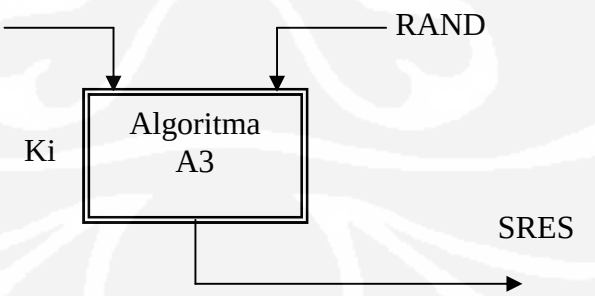
Rancang bangun simulasi ini dibuat dengan algoritma A3 menggunakan kompresi struktur kupu-kupu (*Butterfly structure*) bertujuan untuk mencoba memproses kunci rahasia, Ki untuk tidak terbaca dengan mudah oleh pengguna yang tidak berhak sehingga terhindar dari terjadinya pengkloningan saat melakukan proses membangkitkan nilai SRes (*Signal Response*) atau autentikasi pengguna.

Simulasi ini dibuat untuk mencoba membuat pengolahan algoritma A3 yang sudah ada sebelumnya berbasis komputer mengunakan kompresi yang berbeda seperti *adavtife huffman*, menjadi berbasis mikrokontroller AT89S52 menggunakan kompresi struktur kupu-kupu, walaupun sebenarnya dalam hal kecepatan pengolahan data, kompresi ini lebih efektif dijalankan menggunakan komputer, tetapi dalam hal efektif penggunaan di kondisi apapun, modifikasi menggunakan mikrokontroller lebih efektif.

Modifikasi yang diharapkan dalam penggunaan mikrokontroller adalah mikrokontroller mampu menjalankan program algoritma A3 dengan proses *stand alone* atau tidak tergantung dengan program pembuat serta sistem kerja mikrokontroller dalam mengendalikan komputasi data dari parameter autentikasi GSM mendekati sistem kerja yang sama pada *hand phone* yang mengendalikan komputasi data yang tersimpan di memori SIM card.

Kondisi sekarang sistem keamanan GSM pada area autentikasi pengguna meggunakan algoritma A3 dengan pengolahan parameter-parameter autentikasi lebih komplek, aman dan pengolahan data yang cepat, dinamakan COMP 128-4 berdasarkan AES (*Advanced Encrryption Standart*), dibawah pengembangan oleh 3GPP (*3rd Generation Partnership Project*) yang merupakan kelompok peneliti dari pengembangan autentikasi dan *kriptograpy* khususnya algoritma GSM- *MILENAGE*.

Algoritma A3 merupakan algoritma yang digunakan untuk menghasilkan parameter-parameter autentikasi tersebut



Gambar 1.1 Proses komputasi SRes [2]

Pemrosesan autentikasi GSM dipresentasikan pada Gambar 1.1 dilakukan di simcard agar tidak terdapat sandi rahasia lain yang diperlukan berada di luar simcard.

Salah satu cara yang efektif untuk dapat memahami serta menganalisa proses autentikasi diperlukan suatu alat bantu yang mensimulasikan keadaan yang sebenarnya yaitu mikrokontroller AT89S52 yang menggunakan bahasa *basic compiler* 8051 dan bahasa mesin assembler. Bahasa simulasi yang digunakan dalam rancang bangun simulasi ini menggunakan *basic compiler* dikarenakan lebih mudah dipahami, syntax lebih sederhana dan program yang menggunakan bahasa *basic compiler* 8051 lebih sedikit memakan memori dibanding bahasa assembler.

Alat bantu simulasi yang telah ada sebelumnya menggunakan komputer dengan bahasa pemrograman C, Alat bantu simulasi komputer dengan bahasa pemrograman C mampu mensimulasikan program dalam komunikasi dua arah antara autentikasi GSM pada sisi pelanggan dengan autentikasi GSM pada sisi jaringan dalam satu alat bantu simulasi yaitu komputer.

AT89S52 merupakan kode pabrikasi yang mempunyai kapasitas memori tersendiri, kode pabrikasi yang saat ini telah ada selain AT89S52 yaitu AT89S51 dan AT 89S53 dengan kapasitas memori (RAM *Interna*l) berbeda-beda [8]. Kode pabrikasi dengan kapasitas memori yang mampu mengatasi kebutuhan kapasitas memori yang diinginkan dalam perancangan ini yaitu menggunakan mikrokontroller AT89S52 dengan kapasitas memori 8 kbyte.

1.2 TUJUAN TUGAS AKHIR

Tujuan dari tugas akhir ini adalah sebagai berikut;

1. Merancang bangun simulasi autentikasi GSM menggunakan mikrokontroller.
2. Menguji coba hasil dari komputasi parameter-parameter autentikasi GSM menggunakan mikrokontroller untuk mendapatkan keamanan di komunikasi bergerak.

1. 3 BATASAN MASALAH

Rancang bangun Autentikasi GSM dengan algoritma A3 menggunakan mikrokontroller AT89S52 merupakan simulasi yang dirancang berdasarkan konsep teori keamanan komunikasi GSM yang telah ada. Karena cakupan keamanan komunikasi GSM cukup luas, agar tidak terlalu melebar, untuk itu pembahasan menitikberatkan pada batasan masalah sebagai berikut;

a) Rancang bangun simulasi tidak mensimulasikan algoritma keamanan GSM A8 dan algoritma A5.
b) Rancang bangun mensimulasikan proses autentikasi dengan algoritma A3 yang terdapat pada SIM (S*ubscriber identity module)* card sehingga menghasilkan Sres (S*ignal response).*
c) Simulasi A3 (*Algorithm Function for Authentication*) beroperasi sebagai suatu fungsi yang bersifat searah, dimana dengan mengetahui Rand dan Ki maka SRes dapat diketahui, tetapi tidak bisa dilakukan pembuktian hasil dengan mengetahui *output* sehingga *input* Ki atau Rand diperoleh dengan mudah.
d) Rancangan secara keseluruhan terdiri dari perangkat keras (*hardware)* dan sistem perangkat lunak (*software),* yaitu:
    1. Pada bagian *hardware* blok pengolah data (mikrokontroller AT89S52) dengan input keypad 4X4, tampilan proses simulasi akan terlihat di LCD 2 X 16. Pada proses pembacaan dan pengiriman parameter autentikasi akan berupa byte heksa di data Ki (*Individual Subcriber Authentication Key*), *sinyal response* (SRes). Ki (*Individual Subcriber Authentication Key*).
    2. Pada bagian perangkat lunak (*software*), mengingat adanya proses kemudahan dalam merancang suatu simulasi, maka bahasa pemrograman kompiler BASCOM-8051 yang tepat dipakai. Menu help pada menu barnya memberikan bantuan kemudahan mengatasi instruksi-instruksi yang diperlukan.

1.4 SISTEMATIKA PENULISAN

Pada Tugas akhir ini terdiri dari 5 (Lima) bab, dimana masing-masing bab mempunyai kaitan satu sama lain, yaitu:

BAB 1: Pendahuluan

Memberikan latar belakang tentang permasalahan, tujuan, masalah dan batasan masalah yang dibahas dalam tugas akhir ini.

BAB 2: Autentikasi GSM

Memberikan tinjauan pustaka yang berkaitan dengan sistem arsitektur GSM dan autentikasi GSM, khususnya pada autentikasi pada pelanggan. Membahas teori dasar yang menunjang perancangan sistem termasuk diantaranya dasar-dasar mikrokontroller AT89S52. Selain itu, juga dijelaskan secara singkat *pin out* simcard.

BAB 3: Perancangan sistem dan Perancangan perangkat lunak

Membahas perancangan sistem. Antara lain mengenai sistem algoritma A3, pengolahan data dari triplet – triplet autentikasi GSM sehingga menghasilkannya SRes dan perancangannya.

BAB 4: Perancangan Perangkat Keras

Membahas perancangan sistem dari sisi perangkat keras yang digunakan, disertai prinsip kerja dari perangkat keras tersebut.

BAB 5 : Uji Coba dan Analisa

Menampilkan hasil uji coba disertai analisa dari komputasi triplet – triplet autentikasi GSM.

BAB 6: Kesimpulan

Berisikan beberapa kesimpulan dari dasar-dasar sistem dan perancangan sistem.

BAB 2
AUTENTIKASI GSM

Dalam rekomendasi GSM yang tersusun oleh ETSI *(European Telecommunication Standart Institute)* yang terdiri atas 130 rekomendasi, dimana rekomendasi ini kemudian dapat dibagi menjadi 12 kategori umum, salah satunya mendefinisikan tentang arsitektur fungsional untuk jaringan radio seluler digital.

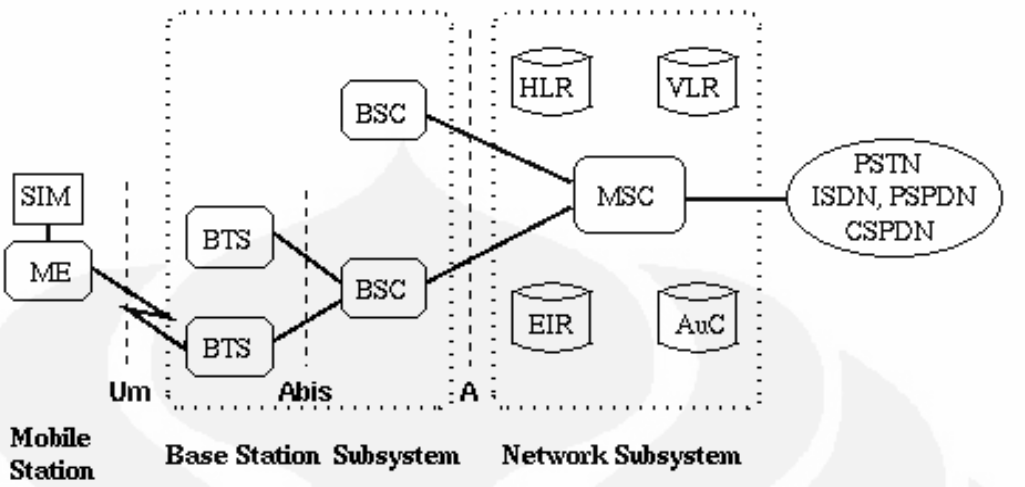
Untuk menerapkan kesatuan fungsional ini kedalam konfigurasi jaringan secara fisik merupakan pekerjaan yang sulit serta melibatkan beberapa perspektif yang berbeda-beda, dengan cara mengintegrasikan beberapa identitas fungsional ke dalam satu node atau dengan mengeksploitasi efek trunking yang selanjutnya disebut juga dengan sistem GSM sedangkan implementasi fisiknya disebut dengan jaringan *global sistem for mobile communication* (GSM).

2.1 JARINGAN *GLOBAL SISTEM FOR MOBILE COMMUNICATION* (GSM)

Global Sistem for Mobile communication (GSM) adalah sebuah standar global untuk komunikasi bergerak digital. GSM adalah nama dari sebuah group standarisasi yang dibentuk di Eropa tahun 1982 untuk menciptakan sebuah standar bersama telpon bergerak selular di Eropa yang beroperasi pada daerah frekuensi 900 MHz. GSM saat ini banyak digunakan di negara-negara di dunia. Jaringan GSM dibagi tiga bagian yaitu:

1. *The base subscriber carries the mobile station. (MS)*
2. *The base station subsystem.*
3. *The network subsystem.*

Gambar 2.1 lay-out keseluruhan arsitektur jaringan dari sistem *global system for mobile communication* (GSM).



Gambar 2.1 *Layout generic* dari jaringan GSM menurut John's Scourias [3]

Keterangan Gambar 2.1:

- (ME)/HP = Mobile Equipment	- SIM =Subscriber Identification Module
- BTS = Base Transceiver Station	- BSC = Base Station Controller
- MSC = Mobile Service Switching Centre	- HLR = Home Location Register
- VLR = Visitors Locations Register	- EIR = Equipment Identity Register
- AuC = Authentication Center	- PSTN = Public Switched Telepone network
- ISDN =Integrated Service Digital Network	

2.1.1 *MOBILE STATION* (MS)

MS merupakan perangkat *outstation* yang biasanya berupa pesawat telepon, yang digunakan pelanggan untuk mendapatkan pelayanan dari jaringan GSM tertera pada Gambar 2.2 yang terdiri dari:

Gambar 2.2 Bagian dari pembentuk *Mobile Station* (MS) [4]

a) *Mobile Equipment* (ME)

ME adalah perangkat yang berupa pesawat teleponnya, serta berfungsi sebagai:

- Unit kontrol, yaitu peralatan di mana pelanggan dapat memilih nomor-nomor yang akan dikirim,
- Unit *transceiver*, yang berfungsi menghubungkan MS dengan BSS melalui hubungan radio dua arah.

Setiap ME memiliki *International Mobile Equipment Identity* (IMEI) yang digunakan untuk mencegah penggunaan perangkat ME yang mengalami suatu pencurian.

b) *Subscriber Identity Module* (SIM) *card.*

SIM card merupakan smart card di mana di dalamnya terdapat microprosessor (umumnya 8 bit), RAM, ROM dan EPROM, sehingga selain menyimpan data dapat pula melakukan proses komputasi [5]. Jika kita melihat dimensi fisiknya, maka dikenal 2 macam SIM card, yaitu IC card SIM (memenuhi standard ISO-7816) yang memiliki ukuran sebesar kartu kredit dan *plug-in* SIM yang memiliki ukuran 15 x 25 mm.

SIM card berfungsi sebagai Unit Logic, yaitu merupakan pengontrol utama terhadap peralatan MS dan digunakan untuk menyimpan informasi untuk mendukung operasi dan pelayanan sistem GSM yang berhubungan dengan proses autentikasi pelanggan. SIM card berisi nomor khusus dari pelanggan yang disebut *International Mobile Subscriber Identity* (IMSI).

Untuk keperluan keamanan, SIM card juga melakukan mekanisme pengecekan keabsahan antara pemakai dengan MS dengan menggunakan PIN (*Personal Identification Number)* atau CHV (*Card Holder Verification)*. Demi alasan keamanan, PIN dapat diganti oleh pemakai jika PIN yang lama sudah diketahui oleh orang lain.

Pemakai harus memasukkan serangkaian digit (biasanya 4-8 digit) untuk dapat memakai perangkat MS-nya. SIM card akan membandingkan digit tersebut dengan data PIN yang tersimpan dalam SIM. Jika sama maka pengaksesan dapat dilanjutkan, sedangakan jika berbeda akan diberi kesempatan tiga kali mencoba dan jika tidak sama juga, maka SIM card akan diblok. Pembukaan *blocking* dapat

dilakukan oleh pemakai dengan menggunakan fasilitas PUK (*Personal Unblocking Key)*. Pembukaan *blocking* dibatasi sampai sepuluh kali dan setelah itu SIM card tidak dapat dipakai lagi sehingga harus diganti dengan yang baru.

Sebagai tambahan untuk keperluan pengecekan otoritasi pelanggan tersebut, maka SIM card harus menyediakan kapabilitas penyimpanan informasi tentang PIN (*Personal Identity Number*), *indicator enable/disable* PIN, peghitungan kesalahan PIN, PUK (*Personal Unblocking Key*), data autentikasi.

2.1.2. BSS *(BASE STATION SUB-SISTEM)*

BSS (*Base Station Sub-Sistem)* merupakan stasiun pemancar atau penerima radio untuk menjangkau (mengcover) satu wilayah kecil yang disebut sell (*cellsite*), BSS terdiri dari dua perangkat yaitu BSC (*Base Station Controller)* dan BTS (*Base Transceiver Station*). Antara BTS dan BSC dihubungkan oleh Abis interface.

a. BSC (*Base Station Controller)*

Fungsi utamanya adalah melakukan pengaturan atau pengontrolan akibat adanya mobilitas pelanggan yang biasanya berpindah-pindah dari satu sel ke sel yang lain. Selain itu juga mengatur terjadinya proses handover pada MS.

b. BTS *(Base Transceiver Station)*

BTS biasa juga dikenal sebagai *Radio Base Station* (RBS). Fungsi utamanya adalah untuk melengkapi keperluan stasiun basis radio pemancar dan penerima. BTS dapat terdiri dari hanya satu pemancar dan penerima atau lebih, tergantung kebutuhan kapasitas trafik. BTS memiliki peralatan yang diperlukan untuk mencakup satu atau lebih wilayah radio (sel).

2.1.3 NSS (*NETWORK AND SWITCHING SUB- SISTEM)*

NSS (Network and Switching Sub-sistem) adalah sistem penyambungan utama dari sistem GSM yang mengatur hubungan komunikasi antara pelanggan GSM dengan sesamanya, ataupun dengan pelanggan baru jaringan telekomunikasi lainnya. Ada lima fungsi pokok dalam NSS, yaitu :

a. MSC *(Mobile Service Switching Center)*

MSC (*Mobile service switching centre)* berperan dalam menyelenggarakan semua fungsi-fungsi penyambungan, pengaturan trafik, pensinyalan dan pembebanan biaya percakapan yang diperlukan untuk MS (*mobile station)* yang berada pada MSC *service area*. Dalam penanganan permintaan panggilan MSC dapat mengakses informasi dari ketiga database yaitu HLR, VLR dan AuC. Setelah menggunakan ketiga data base tersebut maka MSC akan mengup-date ketiga data base tersebut sesuai informasi terakhir dari status panggilan dan posisi panggilan. MSC juga harus dapat berperan sebagai *interface* antara jaringan GSM dengan jaringan lainnya (sebagai gateway MSC).

b. HLR *(Home Location Register)*

HLR (*Home Location Register)* adalah basis data utama yang menyimpan data posisi atau lokasi aktual dari pelanggan. Dua macam data yang tersimpan di HLR adalah:

- Informasi layanan pelanggan, seperti data tentang *teleservices*, *bearer services* dan *supplementary service*.
- Informasi lokasi, untuk melayani permintaan VLR tentang alamat pelanggan yang dianggap baru.

Selain itu, pada HLR juga disimpan dua nomor identitas pelanggan:

- IMSI (*International mobile sub-scribers identity)*, yaitu nomor identitas pelanggan pada jaringan GSM

- *Mobile station* ISDN number (MSISDN), yaitu nomor identitas pelanggan pada perencanaan penomoran PSTN / ISDN.

c. VLR *(Visitors Location Register)*

VLR *(Visitors Location Register)* adalah basis data yang memuat informasi lengkap mengenai seluruh MS yang memasuki wilayahnya. VLR dapat dianggap sebagai data base pelanggan yang dinamik yang secara intensif bertukar informasi dengan HLR. Di samping itu, VLR berfungsi untuk melaksakan proses autentikasi di dalam menangani sewaktu akses panggilan (*call setup*) yang dilakukan oleh seseorang pelanggan dalam wilayah pelayanannya.

d. AUC *(Authentication Centre)*

AUC *(Authentication Centre)* berfungsi melayani HLR dengan menyampaikan parameter autentikasi (*Authentication*) dan pengkodean (*encryptio*n) serta kunci-kunci pengkodean (*ciphering keys*) berdasarkan nomor-nomor yang diberikan, untuk menjamin kerahasiaan setiap panggilan (*call setup*) dan menaikkan tingkat keamanannya.

e. EIR (*Equipment Identity Register*)

EIR (*Equipment Identity Register)* adalah basis data yang memuat informasi tentang identitas dari setiap ME. EIR ini digunakan oleh MSC untuk memeriksa keabsahan identitas dari ME yang sedang digunakan oleh pelanggan, sehingga dapat mencegah kemungkinan seseorang yang tidak berhak atau bukan pemilik ME tersebut *(black list*) untuk menggunakannya.

2.2 KARAKTERISTIK SISTEM KEAMANAN PADA GSM

Sistem keamanan yang terdapat di dalam PLMN-GSM dimaksudkan untuk melindungi jaringan dari suatu pengaksesan yang tidak sah dan menjamin

kerahasiaan para pengguna jasa (pelanggan) GSM. Beberapa aspek yang perlu diperhatikan menyangkut karakteristik keamanan yang terdapat dalam sistem GSM tersebut, antara lain:

- *Mobile subscriber identity authentication*
- *Signalling data confidentiality*
- *User data confidentiality*
- *Mobile subscriber identity confidentiality*

Proteksi dalam jaringan GSM dimulai dari pencegahan penggunaan perangkat (*outstation*) oleh orang yang tidak memiliki otoritas (melalui pengecekan SIM card serta EIR), setelah itu autentikasi terhadap otoritas pelanggan mulai dilakukan seorang pelanggan akan menggunakan sistem. Sebelum suatu proses *call setup* dilakukan, pelanggan (s*ubscriber*) terlebih dahulu harus memberikan identitasnya kepada sistem.

Hal lain yang memerlukan proteksi adalah informasi pensinyalan (*signalling*). Selama pensinyalan berlangsung antara MS dengan jaringan, sistem mengindikasikan suatu prosedur pengkodean informasi (*ciphering mode setting*) yang berarti semua pensinyalan ditransmisikan dalam modus proteksi, demikian halnya dengan data dan pembicaraan (*user data*) yang ditransmisikan dan diterima oleh MS. Proteksi semacam ini merupakan salah satu *features* yang ditawarkan dalam sistem GSM.

Untuk alasan privasi juga diterapkan mekanisme proteksi identitas pelanggan pada jalur radio (*radio path*). Pada MS diberikan identitas sementara yang hanya berlaku bagi wilayah tertentu, di mana apabila memasuki wilayah lain akan diberikan identitas sementara yang baru. Dengan pemberian identitas tersebut maka tidak dimungkinkan untuk menjejaki aktifitas (lokasi) dari suatu MS tertentu.

Apabila keperluan pengamanan tersebut dapat dipenuhi oleh semua perangkat MS dan jaringan, maka hal ini akan menghilangkan kemungkinan penggandaan yang illegal baik pada sistem maupun pada perangkat MS. Agar penggunaan sistem menjadi fleksibel dan efisien, maka informasi pribadi (*personal information mobile subscriber*) dan informasi lain disimpan dalam unit khusus, yaitu *Subsciber Identity Module* (SIM).

2.3 PEMAHAMAN AUTENTIKASI

Autentikasi merupakan prosedur yang digunakan untuk memeriksa keabsahan identitas pelanggan GSM yang mengakses jaringan GSM dan akan menggunakan semua fasilitas layanan (*features*) yang ditawarkan oleh jaringan GSM tersebut. Fungsi utama dari proses autentikasi ini antara lain:

1. Memproteksi jaringan GSM dari suatu usaha pengaksesan oleh seorang pemakai yang tidak sah dan tidak memiliki otoritas.
2. Melindungi privasi pelanggan dari usaha pengaksesan oleh seorang/suatu pihak yang tidak berwenang *(intruder*).
3. Melindungi data yang ditransmisikan pada jalur radio selama pelanggan sedang melakukan hubungan komunikasi dengan sub-sistem radio.

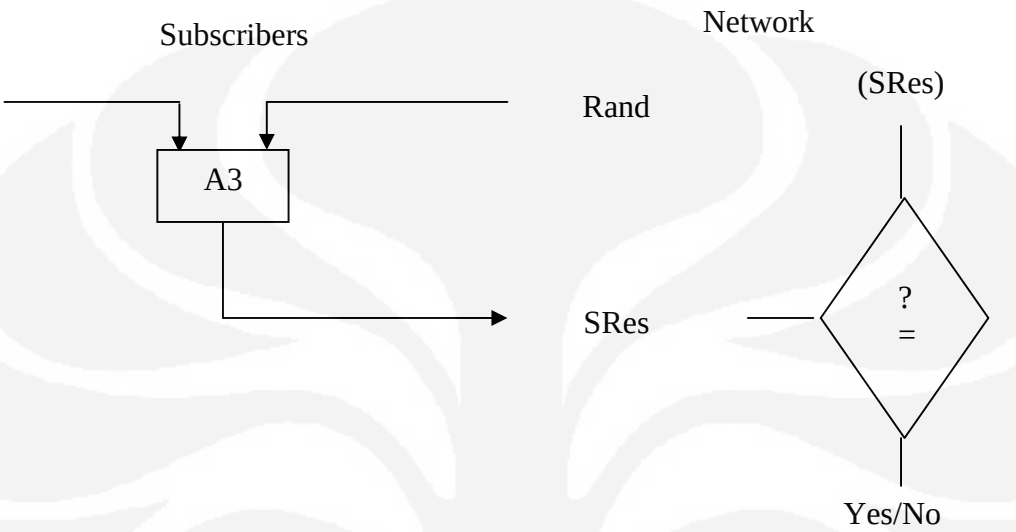
Proses autentikasi mulai dilaksanakan apabila terdapat suatu usaha, yang mana dilakukan oleh seorang pelanggan (MS) untuk mencoba melakukan pengaksesan terhadap jaringan GSM, yang antara lain berupa aktifitas:

- Usaha mengadakan hubungan pembicaraan (*call setup*)
- Pembaharuan lokasi *(location update*) pada pendaftaran lokasi (*location registeration*).
- Mobilitas pelanggan dalam jaringan GSM berupa *handover* maupun *roaming.*
- Pengaktifan fasilitas layanan tambahan (*supplementary services*) tanpa adanya suatu usaha pembangunan hubungan pembicaraan (*call setup*).
- Pertukaran pesan-pesan pendek (SMS).

2.3.1 PRINSIP DASAR AUTENTIKASI

Untuk menghindari adanya penggunaan identitas seorang pelanggan yang sah oleh pihak lain yang tidak berhak dan juga suatu bentuk manipulasi, maka dibuat suatu mekanisme pembuktian keabsahan identitas pelanggan atau autentikasi (*authentication*).

Setiap pelanggan diberikan sebuah modul (*Subscriber Identity Module,*SIM) yang berisi mengenai *International Mobile Subscriber Identity* (IMSI), *Individual Subscriber Authentication Key* (Ki) dan *Authentication Algorithm* (A3)



Gambar 2.3 Prinsip dasar prosedur autentikasi pada jaringan GSM

Secara umum Gambar 2.3 dapat di uraikan sebagai berikut:

Apabila MS akan mengakses sistem GSM, sistem akan memeriksa identitas MS tersebut di atas. Sistem mengirimkan/mentransmisikan RAND (Bilangan acak) yang akan diterima oleh MS. ME meneruskan RAND ke SIM card, yang mana akan memproses bilangan acak tersebut dengan menggunakan Ki yang tersimpan dalam SIM card tersebut sehingga akan menghasilkan suatu sinyal respon SRes (S*ignal Response*) berdasarkan RAND, Ki dan Algoritma A3

MS kemudian mengirimkan SRES ke sistem, dan sistem akan membandingkan SRES ini dengan hasil perhitungannya sendiri (SRes dari sistem) dan apabila sama maka dinyatakan proses autentikasi berhasil yang berarti dapat dilakukan proses selanjutnya. Sebaliknya apabila proses autentikasi dinyatakan tidak berhasil, hubungan terputus dengan suatu indikasi pada MS bahwa autentikasi tidak berhasil. Untuk alasan keamnan, pemrosesan SRes dilakukan dengan SIM, dengan demikian tidak terdapat sandi rahasia lain yang diperlukan berada di luar SIM.

2.3.2 PARAMETER – PARAMETER AUTENTIKASI.

Faktor utama yang perlu diperhatikan secara seksama dalam keseluruhan mekanisme pengamanan, khususnya proses autentikasi, dari proses *features security* yang ditawarkan oleh sistem GSM adalah parameter-parameter autentikasi yang harus diproteksi dengan baik untuk menghindari adanya suatu manipulasi/pemalsuan (*fraudness*). Parameter-parameter tersebut terdiri dari:

a. Ki (Kunci Autentikasi)

Ki (*Individual Subscriber Authentication Key*) merupakan parameter rahasia yang menjadi dasar (*converstone*) dari keseluruhan mekanisme pengamanan, sehingga harus diproteksi dengan baik. Bahkan pelanggan tidak mengetahui nilai Ki yang tersimpan dalam SIM card-nya. Di dalam database pelanggan, Ki disimpan dengan bentuk terkodekan/acak (*encrypted*) untuk mencegah adanya manipulasi/pemalsuan. Ki mempunyai ukuran maksimum sebesar 128 bit.

b. Rand (Bilangan Acak)

Rand (*Random Number*) merupakan suatu parameter yang digunakan untuk memeriksa keabsahan pelanggan (*authorization*). Rand berukuran (maksimal) sebesar 128 bit dan secara acak memiliki nilai yang berkisar dari 0 sampai dengan 2^{128}-1.

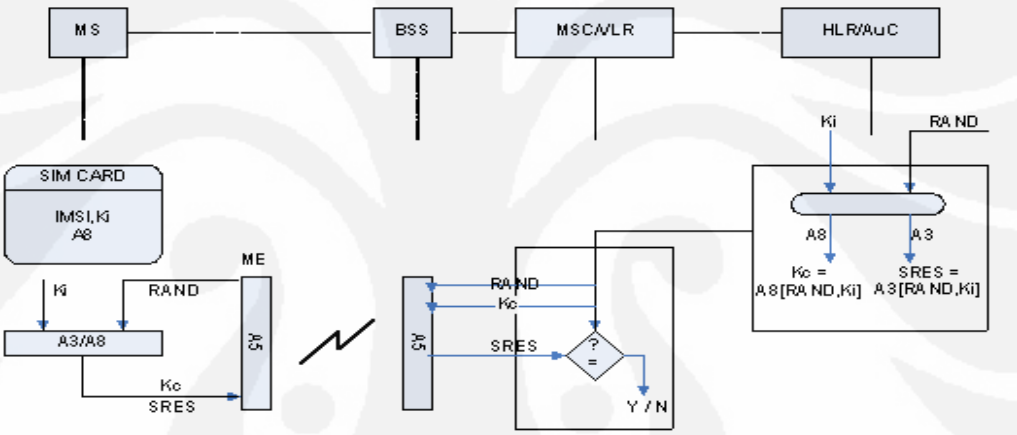
c. SRes (*Sinyal Response)*

SRes (*Signed Response*) didapatkan dari suatu proses komputasi dengan menggunakan algoritma A3, serta Ki dan RAND sebagai parameter-parameter masukan. SRES memiliki ukuran (maksimal) sebesar 32 bit.

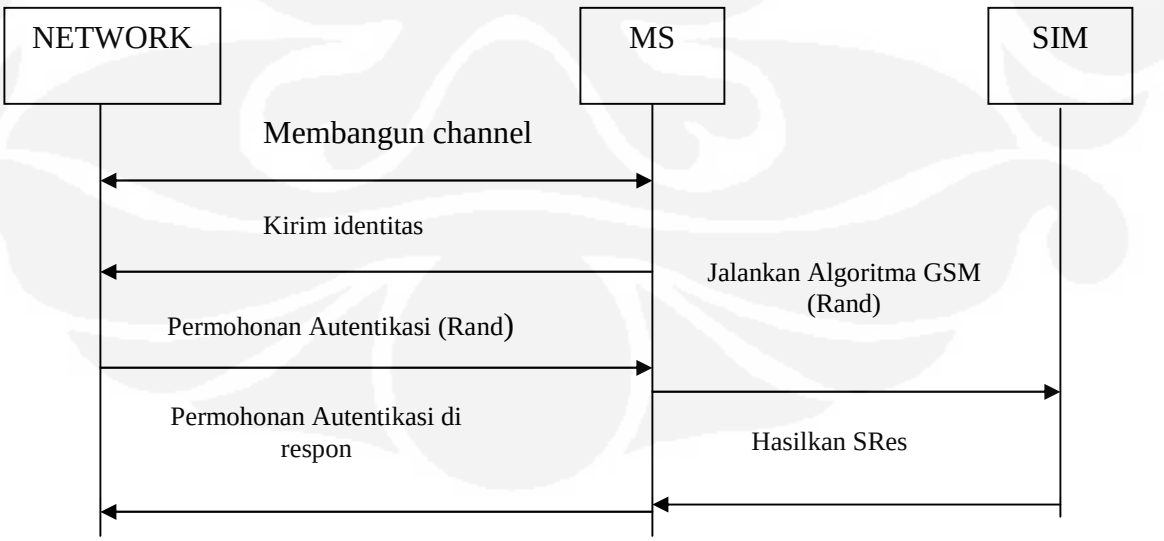
d. A3 (*Algorithm Function for Authentication*)

A3 (*Algorithm Function for Authentication*) beroperasi sebagai suatu fungsi yang bersifat searah (*one-way / trap-door function*), di mana dengan mengetahui Rand dan Ki, maka SRes dapat dihitung dengan mudah; tetapi tidak demikian sebaliknya. Hal ini dimaksudkan agar dapat diperoleh suatu tingkat keamanan yang tinggi. Karena algoritma A3 ini tidak dispesifikasikan secara khusus/mendetail di dalam ETSI Spesifications, maka pemilihan dari design strukturnya tergantung pada masing-masing operator jaringan GSM tersebut (*Independent*).

2.3.3 MEKANISME PROSES AUTENTIKASI



Gambar 2.4. Mekanisme autentikasi antara MS dengan sistem GSM [6].



Gambar 2.5 Diagram proses autentikasi GSM antara MS dengan Network [6]

Gambar 2.4 dan Gambar 2.5 merupakan proses terjadinya suatu sistem autententikasi GSM terjalin antara pengguna layanan GSM dengan jaringan, Pertama-tama pada saat MS / pelanggan melakukan akses ke jaringan GSM, maka sistem akan mengirimkan atau mentransmisikan bilangan acak (Rand) berkapasitas maksimum 16 byte. Kemudian, Rand tersebut akan diterima oleh MS, lalu ME (*Mobile Equipment*) akan meneruskannya ke SIM card yang akan menjalankan run GSM Algoritma untuk memproses bilangan acak tersebut. Dengan kata lain, bahwa di dalam SIM card akan dilakukan komputasi terhadap data masukan berupa Rand yang dipadukan dengan Ki yang sudah terdapat pada SIM card itu. Lalu, input berupa Rand dan Ki akan diproses secara algoritma A3. Maka akan ada ouput berupa SRes berkapasitas 4 byte.

SRes = A3[RAND,Ki]……(2.1)

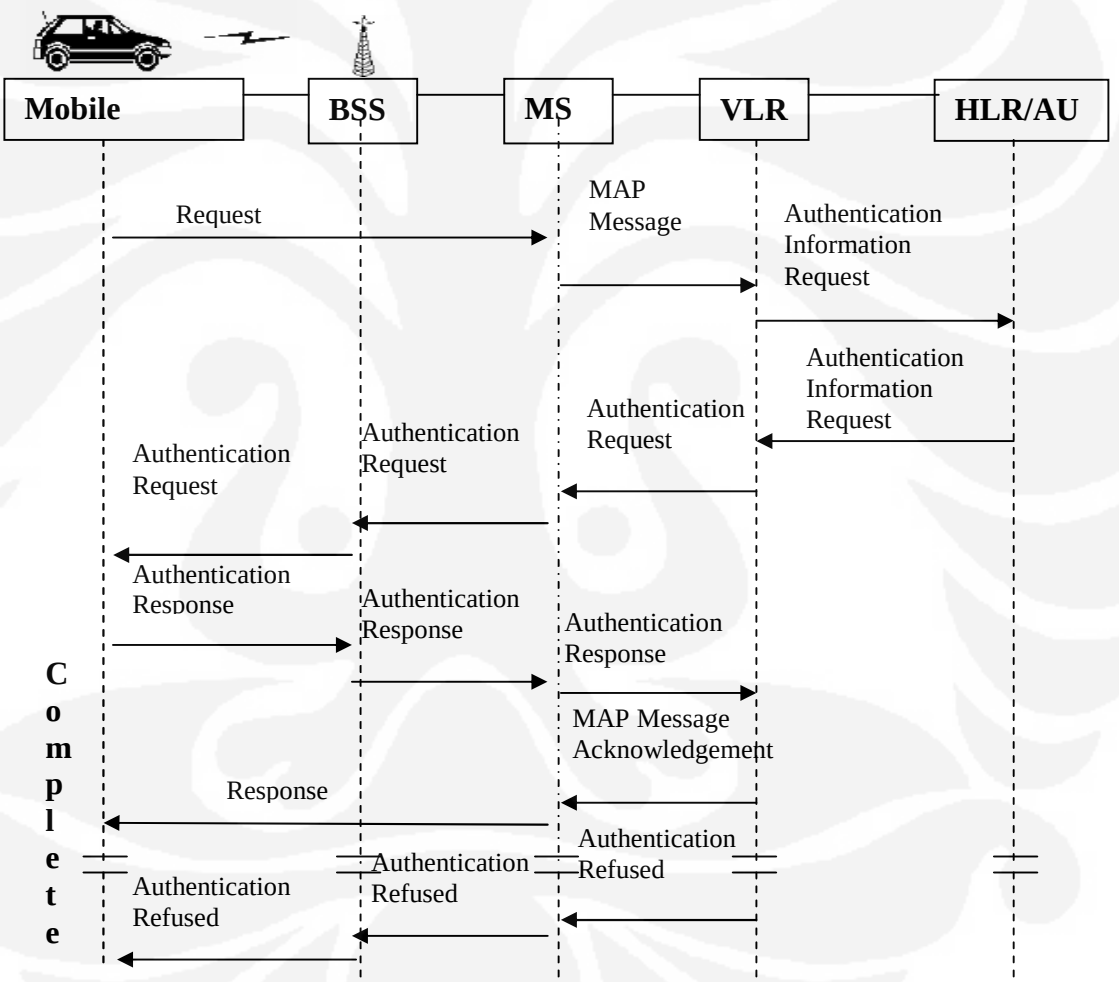
Sistem akan membandingkan kedua SRes tersebut dalam VLR, dimana apabila identik maka proses autentikasi dinyatakan berhasil autentikasi dinyatakan berhasil yang berarti dapat dilanjutkan dengan proses berikutnya. Sebaliknya jika ternyata berbeda, maka proses autentikasi dinyatakan tidak berhasil dan akses ke jaringan GSM akan ditolak. Proses perbandingan kedua SRES ini merupakan bagaian yang utama dari keseluruhan proses autentikasi.

1.3.4 SISTEM PENSINYALAN PADA PROSES AUTENTIKASI GSM.

Selama proses autentikasi dilaksanakan, maka prosesdur transfer pensinyalan yang terjadi/berlangsung pada Gambar 2.6, hubungan interkoneksi (*interface*) antara MS dengan elemen-elemen pendukung jaringan GSM adalah sebagai berikut:

1. Jika MS melakukan akses terhadap jaringan GSM dengan mengirimkan suatu sinyal (*Request*) kepada MSC yang akan diteruskan ke VLR (yang bersangkutan), maka MS tersebut akan (segera) diautentikasi. Proses autentikasi mulai dilaksanakan setelah VLR menerima pesan *MAP message* dari MSC.

2. Apabila MS tersebut ternyata tidak dikenali oleh VLR, maka pertama-tama VLR tersebut akan meminta parameter autentikasi (*triplets*) terlebih dahulu dari HLR/AUC ataupun dari VLR sebelumnya (dari mana MS tersebut berasal) dengan mengirimkan pesan *authentication Information Request*.
3. VLR kemudia memulai pelaksanaan prosedur autentikasi dengan mengirimkan pesan autentikasi (*Authenticatin Request*) ke MSC. Pesan ini mengandung parameter autentikasi RAND.
4. Parameter autentikasi tersebut (RAND) selanjutnya dikirimkan kepada MS dalam pesan *Authentication Request*.



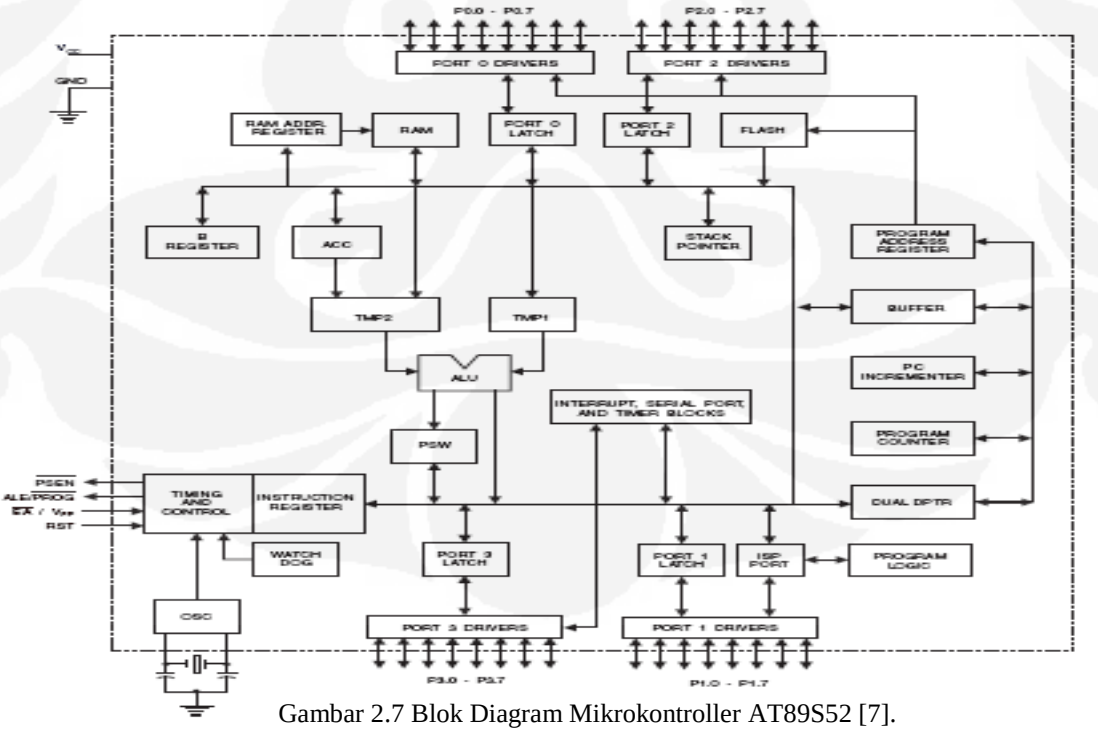
Gambar 2.6 Transfer pensinyalan selama proses autentikasi berlangsung [6]

5. MS akan memberikan respon dengan mengirim balik parameter SRes dalam pesan *Authentication Response*. Untuk pengecekan autentikasi, SRes dikirim dalam pesan *Authentication Response* ke VLR.

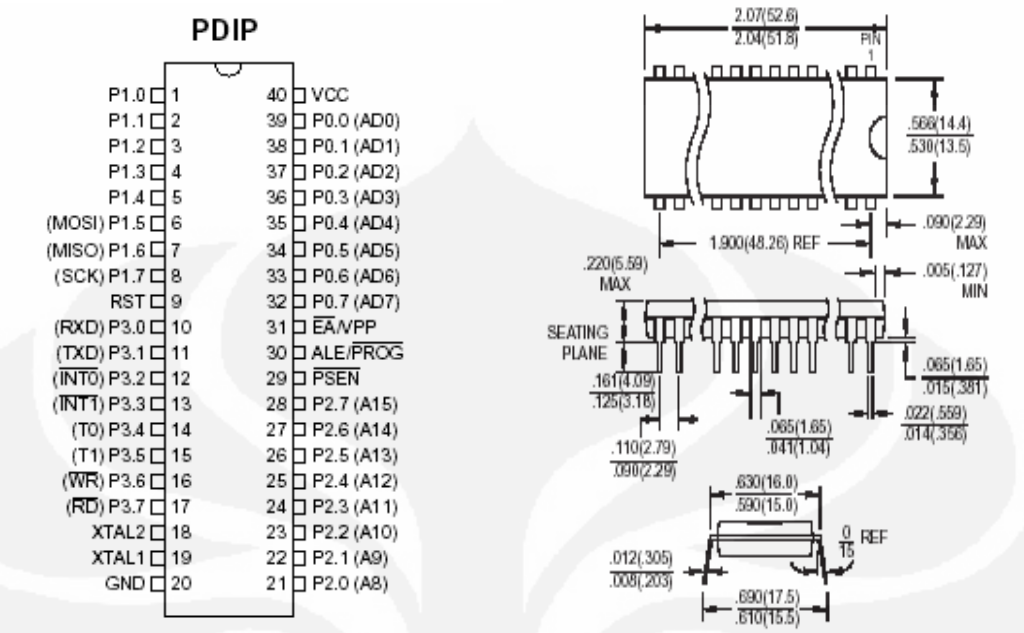
6. Jika keseluruhan proses autentikasi tersebut berhasil dilaksanakan (*Complete*), maka permintaan (akses) yang dilakukan oleh MS tersebut akan dipenuhi, yang diindikasikan dengan pengiriman suatu sinyal (*Response*) dari MSC ke MS.
7. Jika ternyata proses autentikasi terhadap MS tersebut gagal dilaksanakan, maka usaha pengaksesan jaringan GSM oleh MS tersebut ditolak/di batalkan (dindikasikan dengan pesan *Authentication Refused*) yang disertai dengan suatu pemutusan hubungan (sambungan) komunikasi.

2. 4 MIKROKONTROLLER ATMEL AT89S52

Mikrokontroller adalah suatu untai terintegrasi (IC) atau chip yang bekerja berdasar program dan dirancang secara khusus untuk aplikasi sistem kendali atau monitoring. Gambar 2.7 menjelaskan Mikrokontroller yang tersusun dari CPU, ROM, RAM, *TIMER* dan unit I/O baik serial atau paralel. Mikrokontroller bekerja berdasarkan perintah dalam kode bahasa mesin yang diumpankan ke *flash* PEROM yang ada di dalam chip AT89S52. Program yang ditulis dengan bahasa *Assembly* merupakan program sumber yang belum dapat diterima oleh prosesor untuk diterjemahkan dulu menjadi bahasa mesin dalam bentuk kode-kode biner.



Gambar 2.7 Blok Diagram Mikrokontroller AT89S52 [7].



Gambar 2.8 Konfigurasi *Pena AT89S52*. [7]

AT89S52 merupakan mikrokontroller 8 bit dengan spesifikasi sebagai berikut:

a) Kompatible dengan keluarga mikrokontroller MCS-51.
b) 8 Kbyte *In-sistem Programmable* (ISP) *flash* memori sehingga memiliki kemampuan dapat diprogram sampai 1000 kali pemprograman (baca/tulis).
c) Tegangan kerja 4.0 – 5.5 V.
d) Bekerja pada frekuensi 0 – 33 MHz.
e) Tiga level program *memory lock*.
f) 256 x 8 bit RAM internal.
g) 32 jalur I/O yang dapat diprogram.
h) Tiga buah *Timer/ Counter* 16 Bit.
i) Delapan sumber *interrupt*.
j) Saluran UART serial *Full Duplex*.
k) *Watchdog Timer*.
l) *Mode low-power idle* dan *Power-down*.
m) *Interrupt recovery* dari modul *power-down*.
n) *Dual data pointer*.
o) Mode pemprograman ISP yang fleksible (Byte dan Page Mode).

AT89S52 dirancang dengan logika statis untuk operasi hingga frekuensi nol dan mendukung penyimpangan daya dua buah perangkat lunak (*software*) untuk pemilihan mode operasi. Mode *idle* menghentikan CPU dan membiarkan RAM, *timer/counter*, port serial, dan sistem interupsi untuk terus berfungsi. Mode *power-down* menyimpan isi RAM tetapi membekukan osilator, menon-aktifkan seluruh fungsi *chip* sampai ada interupsi eksternal atau reset pada *hardware*.

2. 4. 1 KONFIGURASI PIN

Mikrokontroller AT89S52 dilengkapi dengan 4 buah port paralel, ditunjukkan pada Gambar 2.8 yaitu ports 0, port 1, port 2, port 3 yang masing-masing port terdiri atas 8 pin. Keempat port ini dapat diakses dengan pengalamatan secara bit.

Port 0 dapat dikonfigurasikan sebagai bus alamat/data bagian rendah *(low byte)* dalam pengaksesan memori data dan memori eksternal. Port 1 merupakan port I/O dua arah yang dilengkapi *pull-up* internal. Port 2 juga dilengkapi dengan *pull-up* internal. Selama pengaksesan memori data eksternal yang menggunakan perintah dengan alamat 16 bit, port 2 akan memberikan byte alamat bagian tinggi *(high byte).* Jika akses memori data eksternal dengan alamat 8 bit, port 2 akan mengirimkan isi dari SFR P2. Sebagai I/O biasa, port 3 mempunyai karakteristik yang sama dengan port 1 dan port 2. Perbedaan port 3 dari port yang lain adalah bahwa port 3 mempunyai fungsi-fungsi alternative seperti pada table 2.1 di bawah ini.

Tabel 2. 1 Fungsi Alternatif Port 3

Nama Pin	Fungsi Alternatif	Keterangan
P3.0	RXD	Port masukan serial
P3.1	TXD	Port keluaran serial
P3.2	INT0	Interupsi eksternal 0
P2.3	INT1	Interupsi eksternal 1
P3.4	T0	Masukan eksternal *Timer* 0
P3.5	T1	Masukan eksternal *Timer* 1
P3.6	WR	Sinyal tanda baca memori data eksternal
P3.7	RD	Sinyal tanda tulis memori data eksternal

Mikrokontroller AT89S52 selain memiliki port – port parallel, piranti ini juga di lengkapi dengan perangkat komunikasi serial. Untuk mengaktifkan dan mengkonfigurasinya, *programmer* harus mengakses register SCON dan bit SMOD (bit ke-7 pada register PCON). Dimana perangkat komunikasi serial pada mikrokontroller AT89S52 dapat dioperasikan dalam 4 mode, yaitu:

a. Mode 0

   Merupakan sarana komunikasi data seri sinkron, data seri dikirim dan diterima melalui kaki RxD, sedangkan kaki TxD dapat dipakai untuk menyalurkan clock yang diperlukan komunikasi data sinkron. Data ditransmisikan per 8 bit dengan kecepatan transmisi data (*Baud rate*) tetap sebesar $^1/_2$ frekuensi kerja AT89S52.

b. Mode 1

   Mode 1 dan dua mode berikutnya merupakan sarana komunikasi seri asinkron. Data seri dikirim melalui kaki TxD dan diterima dari kaki RxD. Data ditransmisikan per 10 bit yang terdiri atas 1 bit start (‘0’), 8 bit data, dan 1 bit stop (‘1’). Kecepatan transmisi data (*baud rate*) ditentukan lewat timer 1 yang bisa diatur untuk berbagai kecepatan.

c. Mode 2

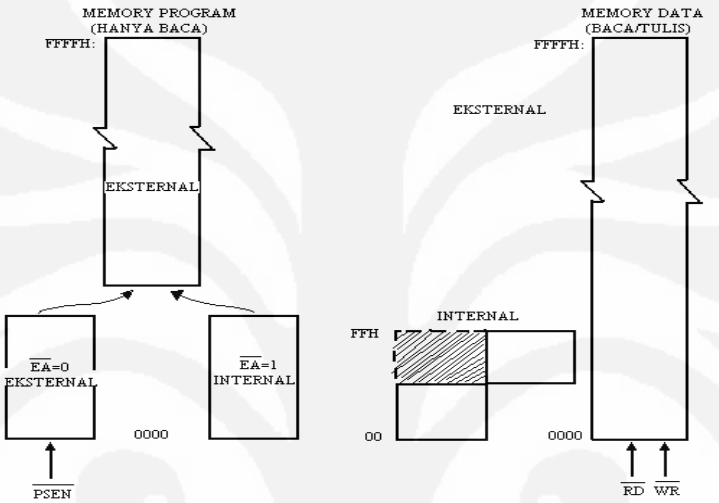
   Data seri dikirim melalui kaki TxD dan diterima dari kaki RxD. Data ditransmisikan per 11 bit, terdiri atas 1 bit start (‘0’), 8 bit data, 1 bit data tambahan (bit ke-9), dan 1 bit stop (‘1’). Kecepatan transmisi data (*baud rate*) hanya dapat dipilih $^1/_{32}$ atau $^1/_{64}$ frekuensi kerja AT89S52.

d. Mode 3

   Data seri dikirim melalui kaki TxD dan diterima dari kaki RxD. Data ditransmisikan per 11 bit juga. Pada dasarnnya mode 2 dan mode 3 sama persis. Perbedaannya adalah kecepatan transmisi data (*baud rate*) mode 3 ditentukan lewat timer 1, yang bisa diatur untuk berbagai kecepatan, persis sama dengan mode 1.

2. 4. 2 ORGANISASI MEMORI

Semua perangkat MCS-51, termasuk AT89S52, memiliki ruang alamat memori data dan program yang terpisah. Dimana Program memori dikhususkan untuk menyimpan program, hanya bisa dibaca, sedangkan data memori untuk menyimpan data-data yang bisa berubah dalam proses, bisa baca dan tulis. Dimana pada Gambar 2. 9 memperlihatkan struktur memory dan data pada AT89S52.



Gambar 2. 9 Struktur memori program dan data pada AT89S52 [8].

Pemisahan memori program dan data tersebut membolehkan memori data diakses dengan alamat 8 bit, sehingga dapat dengan cepat dan mudah disimpan dan dimanipulasi oleh CPU 8 bit. Namun demikian, alamat memori data 16 bit bisa juga dihasilkan melalui register DPTR (*Data pointer*).

a. Memori Program

   Memori program hanya bisa dibaca saja. Terdapat memori program yang bisa diakses langsung hingga 64K byte. Sedangka strobe untuk akses program memori eksternal melalui sinyal PSE (*Program Store Enable).*

b. Memori Data

   Memori data menempati suatu ruang alamat yang terpisah dari memori program. Memori eksternal dapat diakses secara langsung hingga 64K byte dalam ruang

memori data eksternal. CPU akan memberikan sinyal baca dan tulis, selama pengaksesan memori data eksternal.

c. Flash PEROM

Untuk menyimpan program secara permanen, AT89S52 menyediakan *Flash* PEROM dengan kapasitas 4 Kbyte, yaitu suatu ROM yang dapat ditulis ulang atau dihapus menggunakan *programmer.*

d. SFR (*Special Function Register*)

Mikrokontroller mempunyai peta memori yang dikenal sebagai *Special Function Register* (SFR). SFR pada mikrokontroller dibagi menjadi beberapa bagian serta mempunyai alamat masing-masing.

Tidak semua alamat pada SFR digunakan dan diimplementasikan pada chip. Jika dilakukan pembacaan pada alamat yang tidak terpakai tersebut akan menghasilkan data acak dan penulisannya tidak menimbulkan effek sama sekali. Berikut ini adalah beberapa SFR dan alamatnya:

1. Accumulator : Menyimpan data sementara (E0H).
2. Register B : Operasi perkalian dan pembagian (F0H).
3. *Program Status word* (PSW): Informasi Status Program (D0H).
4. *Stack Pointer* : Menyimpan dan mengambil data dari atau ke stack (81H).
5. *Data Pointer* : Menampung data 16 bit (83H dan 82H).Port 0, 1, 2, 3 : Menyimpan data yang akan dibaca atau ditulis dari atau ke port (80H, 90H, A0H).
6. *Serial Data Buffer* : Sebagai register penyangga penerima atau pengirim (99H).
7. *Timer Register* : Merupakan register-register pencacah 16 bit untuk masing-masing timer 0, 1, dan 2.
8. *Capture Register*: Menyimpan nilai isi ulang (CBH dan CAH).

e. Mode-mode pengalamatan

1. Pengalamatan langsung (*Direct Addressing*)

   Dalam pengalamatan langsung, pemindahan data ditentukan berdasarkan alamat 8 bit (1 byte) dalam suatu instruksi. Hanya RAM data internal dan SFR yang dapat diakses secara langsung

2. Pengalamatan tak langsung (*Indirect Addressing*)

   Dalam pengalamatan tak-langsung, instruksi menentukan suatu register yang digunakan untuk menyimpan alamat opeRand. Baik RAM internal maupun eksternal dapat diakses secara tak-langsung. Register alamat untuk alamat-alamat 8 bit bisa menggunakan stack pointer atau R0 atau R1 dari bank register yang dipilih. Sebaliknya, alamat 16 bit hanya bisa menggunakan register pointer data 16 bit atau DPTR.

3. Pengalamatan Terindeks (*Indexed Addressing*)

   Memori program hanya bisa diakses melalui pengalamatan terindeks. Mode pengalamatan ini ditujukan untuk membaca label *look-up* (*look-up tables*) yang tersimpan dalam memori program. Sebuah register dasar 16 bit menunjuk ke awal atau dasar tabel dan akumulator di-set dengan angka indeks tabel yang dapat diakses. Alamat dari entri tabel dalam memori program dibentuk dengan menjumlahkan data akumulator dengan penunjuk awal tabel.

2. 5 DT-51 MINIMUM SISTEM.

DT-51 adalah alat pengembangan mikrokontroller keluarga MCS-51TM yang sederhana, handal, dan ekonomis. DT-51 berbentuk sistem minimum dengan komponen utamanya mikrokontroller AT89S52. DT-51 memungkinkan dalam mengembangkan aplikasi digital dengan mudah; menulis *software* (perangkat lunak) pada komputer yang kemudian men-download ke board DT-51, dan menjalankannya; serta dapat langsung bekerja sendiri (*stand-alone*) pada sistem yang ada tanpa penggantian/penambahan komponen.

Minimum Sistem mikrokontroller merupakan sebuah kit mikrokontroller yang sudah dapat berfungsi sebagai pengontrol utama suatu sistem elektronika. Kit

DT-51 merupakan kit yang lengkap untuk dapat digunakan sebagai board utama karena telah tersedia port serial, input data, memori eksternal 28C64B, dan 1 buah PPI 8255. DT-51 juga telah dilengkapi dengan driver dan port LCD yang memudahkan kita bila ingin menghubungkan LCD ke board. Spesifikasi DT-51 sebagai berikut :

1. Berbasis mikrokontroller AT89S52 yang berstandar industri.
2. Serial port interface standar RS-232 untuk komunikasi antara komputer dengan board DT-51.
3. 8 Kbytes non-volatile memory (EEPROM) untuk menyimpan program dan data.
4. 4 por t input output (I/O) dengan kapasitas 8 bit tiap por tnya.
5. Port Liquid Crystal Display (LCD) untuk keperluan tampilan.
6. Konektor ekspansi untuk menghubungkan DT-51 dengan *add-on board* yang kompatibel dari *Innovative Electronics*.

2. 5. 1 PETA MEMORI DT-51

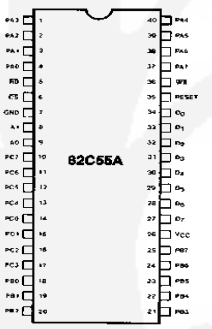
Peta Memori DT-51 menunjukkan alamat masing-masing bagian komponen sebagai berikut :

1. **0000H - 1FFFH**, **8** Kbyte pertama digunakan sebagai internal dan 4 Kbyte PEROM yang berisi kernel code, sedangkan 4K sisanya reserved.
2. **2000H - 3FFFH, 8** Kbyte kedua digunakan untuk PPI 8255 dan hanya terpakai 4 alamat :
    a. 2000H - Port A
    b. 2001H - Port B
    c. 2002H - Port C
    d. 2003H - Control Word Register
3. **4000H - 5FFFH, 8** Kbyte ketiga digunakan oleh EEPROM untuk menyimpan User Code.
4. **6000H – FFFFH,** CS3-CS7 disediakan untuk ekspansi.

Pada memori internal DT-51 sudah diisi dengan kernel yang tidak bisa ditulis ulang kembali. Oleh karena itu, DT-51 menggunakan memori eksternal AT28C64B, yaitu *Electrically Erasable* and *Programmable Read Only Memory* (EEPROM) kualitas tinggi berukuran 64 KByte, yang terdiri dari 8.192 words berukuran 8 bit, sehingga memiliki ukuran program yang lebih besar.

2. 5. 2 PPI 82C55 (*PROGRAMMABLE PERIPHERAL INTERFACE*).

PPI *(Programmable Peripheral Interface)* 8255 adalah komponen antarmuka yang sangat populer serta murah dan merupakan chip antarmuka 24 bit (3 *ports*) yang dapat diprogram kerjanya sesuai keinginan. PPI 8255 merupakan chip yang paling banyak digunakan untuk interfacing komputer yang dihubungkan ke port ISA komputer.



Gambar 2. 10 Pin-Out dari adapter antarmuka peripheral (PPI) 8255 [9].

Pada Gambar 2. 10 merupakan pin kaki IC 8255 yang terdiri dari 40 pin, dimana pin Gnd berada pada pin 7 dan Vcc pada pin ke 26. Berikut ini merupakan deskripsi dari masing-masing pin:

1. PA0 – PA7

   Pin ini merupakan port A yang terdiri dari 8 bit yang dapat diprogram sebagai input atau output dengan *mode bidirectional input/output*.

2. PB0 – PB7

   Port B ini dapat diprogram sebagai input/output tetapi tidak dapat digunakan sebagai port *bidirectional*.

3. PC0 – PC7

   Port C ini dapat diprogram sebagai input/output bahkan dapat dipecah menjadi 2, yaitu CU (bit PC4 – PC7) dan CL (bit PC0 – PC3).

4. RD dan WR

   Sinyal kontrol aktif rendah ini dihubungkan ke 8255. Jika 8255 menggunakan desain peripheral I/O, IOR, dan IOW dari sistem bus, maka akan dihubungkan ke kedua pin ini.

5. RESET

   Pin aktif tinggi ini digunakan untuk membersihkan (clear) control register. Ketika RESET diaktifkan, seluruh port akan diinisialisasi sebagai port input.

82C55 dipilih dari pin CS (*Control Select)* untuk pemprograman dan untuk membaca atau menulis ke suatu port. Pemilihan register dilaksanakan melalui pin – pin masukan A0 dan A1 yang memilih suatu register internal untuk pemprograman atau operasi. Dimana pada Table 2. 2, menunjukkan tugas port I/O yang dipakai untuk memprogram dan mengakses port I/O.

Tabel 2. 2 Pemilihan port I/O untuk 8255 [9].

CS	A1	A0	Fungsi
0	0	0	Port A
0	0	1	Port B
0	1	0	Port C
0	1	1	Control Register
1	X	X	8255 tidak dipilih

Pada saat port A, B, dan C digunakan sebagai I/O, maka mode operasi port tersebut perlu di-set. Ada empat mode operasi yang dimiliki 8255, yaitu:

1) Mode 0 (*Basic input / output*)

   Merupakan mode yang paling sederhana, dimana semua port dapat diprogram sebagai input/output. Pada mode ini seluruh port sebagai output atau input dan tidak ada port ynag dapat dikontrol secara individual.

2) Mode 1 (*Strobe input / output*)

   Pada mode ini port A dan B dapat digunakan sebagai input atau output dengan kemampuan handshaking. Sinyal handshaking disediakan oleh bit-bit port C.

3) Mode 2 (*Bidirectional bus*)

Port A dapat digunakan sebagai port bidirectional I/O dengan kemampuan handshaking, dimana sinyalnya disediakan oleh port C. Port B dapat digunakan sebagai model I/O sederhana atau mode 1 *handshaking*.

4) Mode BSR (*Bit Set / Reset*)

Dengan mode ini, hanya port individual port C saja yang dapat diprogram.

2. 6 KOMUNIKASI SERIAL

Untuk dapat melakukan hubungan dengan perangkat lain, sistem ini dirancang menggunakan salah satu komunikasi data, yaitu komunikasi data serial. Pada prinsipnya, komunikasi serial merupakan komunikasi dimana pengiriman data dilakukan per bit sehingga lebih lambat dibandingkan komunikasi paralel, seperti pada port printer yang mampu mengirim 8 bit sekaligus dalam sekali detak. Adapun keuntungan transfer data secara serial adalah dari jumlah kabel yang digunakan lebih sedikit. Beberapa contoh komunikasi serial seperti mouse, scanner, dan sistem akuisisi data yang terhubung ke port COM1/COM2.

Peralatan Komunikasi port Serial dibagi menjadi dua kelompok pada Tabel 2.3, yaitu DCE (*Data Communication Equipment)* dan DTE (*Data Terminal Equipment)*. Komunikasi serial membutuhkan port sebagai saluran data.Berikut tampilan port serial DB9 yang umum digunakan sebagai port serial. Konektor port serial terdiri dari 2 jenis, yaitu konnektor 25 pin (DB25) dan 9 pin (DB9) yang saling berpasangan. Bentuk dari konnektor DB-25 sama persis dengan port paralel. Umumnya COM1 berada di alamat 3F8H sedangkan COM2 di alamat 2F8H..

Tabel 2. 3 Jenis Sinyal RS-232 yang umum digunakan [8].

NAMA SINYAL	**ARAH SINYAL**	**NOMOR KAKI**	
		DB9	**DB25**
Signal Common	-	5	7
Transmitted data (TD)	Ke DCE	3	2
Received Data (RD)	Dari DCE	2	3
Request to Send (RTS)	Ke DCE	7	4

Clear to send (CTS)	Dari DCE	8	5
DCE Ready (DSR)	Dari DCE	6	6
DTE Ready (DTR)	Ke DCE	4	20
Ring indicator (RI)	Dari DCE	9	22
Data Carrier Detect (DCD)	Dari DCE	1	8

Komunikasi serial pada AT89S52 mempunyai *On Chip Serial Port* yang dapat digunakan untuk komunikasi data serial secara *full duplex* (proses pengiriman data dan penerimaan data dapat terjadi secara bersamaan). Dimana data yang diterima maupun yang akan dikirimkan ditampung terlebih dahulu pada Register SBUF (pada alamat 99H). Register SBUF terdiri atas dua buah register yang menempati alamat yang sama, yaitu:

a) Register Transmit

Register bersifat *write only* yang berfungsi menampung data dari bus internal sebelum dikirimkan melalui port serial.

b) Register Receive

Register bersifat read only yang berfungsi menampung data dari port serial sebelum diteruskan ke bus internal pada saat register SBUF dibaca.

Selain register SBUF, terdapat dua buah register yang berhubungan dengan komunikasi serial, yaitu register PCON (87H) dan register SCON (98H). Bit ke-7 dari register PCON, yaitu SMOD, digunakan untuk mengatur nilai baudrate. Jika SMOD diberi logika 1, maka baudrate akan menjadi dua kali lipat.

Register SCON (*Serial Control*) pada Gambar 2.11 mode operasi port serial mikrokontroller.

7	6	5	4	3	2	1	
SM0	SM1	SM2	REN	TB8	RB8	T1	R1

Gambar 2. 11 Register SCON [8]

Tabel 2. 4 Fungsi – fungsi bit register SCON [8].

SM0	Serial port mode 0, bit pengatur mode
SM1	Serial port mode 1, bit pengatur mode
SM2	Serial port mode 2, bit untuk mengaktifkan komunikasi multiprosesor pada kondisi set.
REN	Receive Enable, REN = 1 enable, REN = 0 disable.
TB8	Transmit bit, bit ke-9 untuk kirim data pada mode 2 dan 3
RB8	Receive bit, bit ke-9 untuk kirim data pada mode 2 dan 3. Pada mode 1, bit berfungsi sebagai stop bit.
T1	Transmitt Interrupt, bit yang akan di set pada saat akhir pengiriman data.
R1	Receive Interrupt, bit yang akan diset pada saat akhir penerimaan data

Dalam operasi komunikasi serial terdapat mode yang dapat diatur oleh register SCON, yaitu dengan mengatur bit SM1 dan SM0. Ada empat buah pilihan mode komunikasi, seperti pada Tabel 2. 5 berikut ini.

Tabel 2. 5 Mode Komunikasi Serial [8]

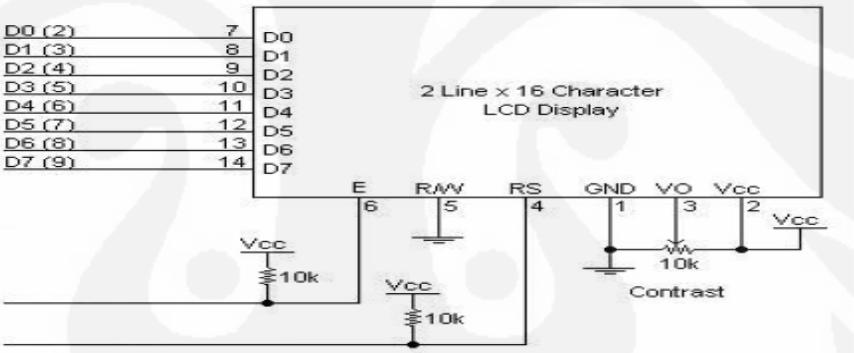
MODE	SM0	SM1	KETERANGAN	BAUDRATE
0	0	0	Shift register 8 bit	F_{osc} / 12
1	0	1	UART 8 bit	Dapat diatur
2	1	0	UART 9 bit	F_{osc} / 16 atau F_{osc} / 32
3	1	1	UART 9 bit	Dapat diatur

2. 7 MODUL LCD (*Liquid Crystal Display*)

Penampil informasi yang lazim digunakan adalah LCD (*Liquid Crystal Display*). LCD yang digunakan adalah LCD Dot Matrik dengan jumlah karakter 16x2. LCD ini nantinya akan digunakan untuk memampilkan informasi koordinat latitude dan longitude, nilai set point (*magnitude*) dan status dari proses. Jenis LCD yang digunakan adalah LCD dari Hitachi tipe H16028B.

Adapun fitur yang disajikan dalam LCD ini adalah:

a. Terdiri dari 16 karakter dan 2 baris
b. Mempunyai 192 karakter tersimpan
c. Terdapat karakter generator terprogram
d. Dapat dialamati dengan mode 8-bit dan 4-bit
e. Dilengkapi dengan *backlight*



Gambar 2.12 LCD 16x2 [10].

Pada Gambar 2.12 LCD terdiri dari 8 jalur data, 3 jalur kendali dan fasilitas pengaturan kontras serta *backlight*. LCD ini dapat dikendalikan dengan mikrokontroller atau mikroposesor.

Deskripsi fungsi-fungsi pin dari penampil LCD ini adalah:

1. VSS, sebagai suplai 0 volt atau ground.
2. VDD, sebagai suplai input untuk LCD (5 volt).
3. VO, sebagai tegangan operasi untuk LCD atau pengaturan kontras layer.
4. RS, sebagai jalur data dan penghantar kode instruksi. (H: DATA, L: kode instruksi.

5. R/W, sebagai jalur baca-tulis data ke mikroprosesor.

6. E, sebagai sinyal *enable* bagi *chip*.

7. DB0-DB7, sebagai data bit 0 sampai dengan data bit 7.

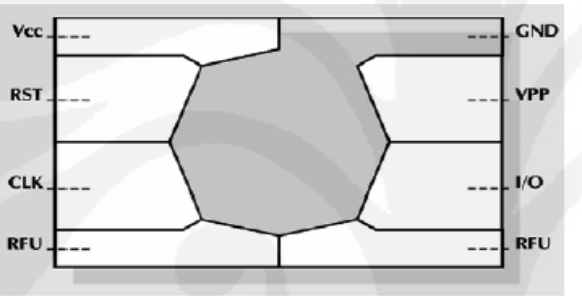
2.8 KONFIGURASI PIN SIMCARD.

Memori pada kartu chip memiliki 2 fungsi dasar:

- Tempat penyimpanan data
- Tempat menjalankan algoritma-algoritma untuk pembuktian identitas pelanggan,

Informasi data tersebut disimpan dalam file data untuk aplikasi khusus.

.



C1	C5
C2	C6
C3	C7
C4	C8

Gambar 2.13 Struktur kontak pada kartu [11]

Fungsi kontak-kontak pada gambar 2.13 diatas adalah :

- C1 digunakan untuk *input power supply* (Vcc) dari piranti antarmuka.
- C2 untuk RST dan digunakan oleh piranti antarmuka untuk mengirim sinyal reset ke mikrosirkit kartu.
- C3 untuk *clock* (CLK) dan sinyal-sinyal pewaktuan dikirimkan ke kartu melalui C3.
- C5 sebagai tegangan referensi (GND), nilai tegangan itu dianggap 0 volt.
- C6 secara bebas digunakan untuk memprogram atau menghapus (Vpp).
- C7 menyelenggaraakan komunikasi ke dan dari kartu, dan disebut I/O.
- C4 dan C8 tidak digunakan.

BAB 3
PERANCANGAN SISTEM
DAN PERANCANGAN SOFTWARE

3.1 SISTEM ALGORITMA A3

Perancangan sistem autentikasi GSM dengan algoritma A3 menggunakan mikrokontroller AT 89S52 untuk mampu membaca/mensimulasikan proses autentikasi yang terjadi di simcard.

Mengetahui komputasi data yang terjadi saat proses autentikasi simcard GSM berjalan sehingga digunakan untuk memproteksi jaringan GSM dari suatu usaha pengaksesan oleh seorang pemakai yang tidak sah dan tidak memiliki otoritas

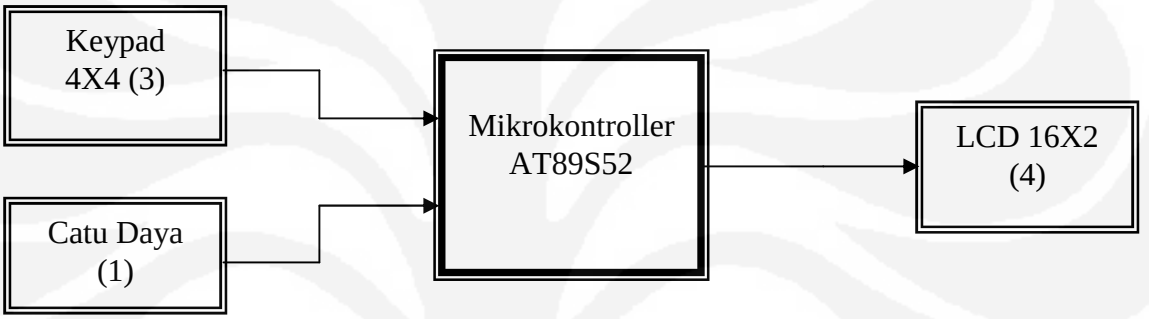
Autentikasi simcard GSM dilakukan agar hanya simcard yang terdaftar dan berhak saja yang dapat menggunakan layanan operator jaringan. Selain itu, digunakan agar tagihan dikenakan pada simcard GSM yang tepat, yang memang memanfaatkan layanan jaringan. Algoritma yang digunakan dalam proses autentikasi simcard layanan pada jaringan GSM adalah algoritma A3. Algoritma ini tidak bersifat publik sehingga hanya antarmuka eksternalnya saja yang dispesifikasikan dalam GSM. Keamanan algoritma ini tergantung pada kunci rahasia *user Ki* yang beririsan antara *mobile phone* dan jaringan GSM. GSM sendiri tidak menspesifikasikan panjang nilai *Ki* sehingga penentuan panjang nilai *Ki* biasanya diserahkan sepenuhnya kepada pihak operator masing-masing. Namun, biasanya panjang kunci yang biasa digunakan oleh operator adalah maksimal 128 bit.

Adapun sistem perancangan autentikasi GSM dengan algoritma A3 menggunakan mikrokontroller AT89S52 secara garis besar adalah sebagai berikut:

- Mikrokontroller membangkitkan sinyal acak (RAND) dengan ukuran sebesar maksimal 128 bit dari database yang tersimpan di memori.
- Mikrokontroller melakukan komputasi data terhadap RAND dan kunci Ki dengan ukuran 128 bit menggunakan algoritma A3 yang terdapat dalam simcard sehingga menghasilkan respon SRes.
- LCD akan menampilkan pernyataan autentikasi terlaksana dengan menampilkan nilai Sres.

3. 2 BLOK DIAGRAM SISTEM AUTENTIKASI SIMCARD GSM

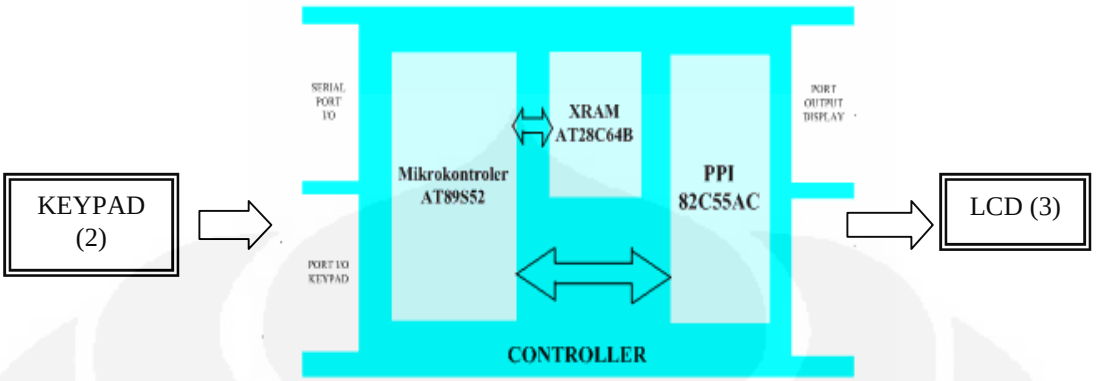
Pada sistem perangkat perancangan ini, akan mengolah informasi data dari perangkat simulasi data dari *keypad* sedangkan output berupa hasil komputasi data di tampilkan di LCD. Pada Gambar 3. 1 dan Gambar 3. 2 merupakan blok diagram dari sistem autentikasi yang akan dibuat.



Gambar 3. 1 Blok diagram sistem autentikasi GSM

Dari gambar blok diagram sistem Gambar 3.1 dapat dijelaskan:

1. Catu daya memberi tegangan masukan sesuai tegangan kerja mikrokontroller sehingga mikrokontroller dapat beroperasi sebagaimana mestinya. Sehingga komunikasi yang terjadi antara catu daya dengan mikrokontroller satu arah.
2. Keypad melakukan komunikasi satu arah dengan mikrokontroller, mikrokontroller menerima instruksi dari keypad baik berupa masukan pembuka password maupun memberikan simulasi masukan data. Keypad juga memberikan perintah instruksi langkah-langkah selanjutnya yang akan dijalankan oleh mikrokontroller
3. LCD sebagai output dari semua proses yang terjadi, menerima masukan saja dari mikrokontroller, baik berupa data proses maupun data hasil akhir dari komputasi data-data yang telah diolah oleh mikrokontroller. Oleh karena itu komunikasi yang terjadi hanya satu arah.



Gambar 3. 2 Diagram sistem pengolahan dan pengirim data yang dikendalikan oleh Mikrokontroller AT89S52

Diagram sistem pengolahan dan pengiriman data yang dikendalikan oleh mikrokontroller terhadap peralatan autentikasi yang lain yang ditunjukkan oleh Gambar 3.2 dapat dijelaskan sebagai berikut:

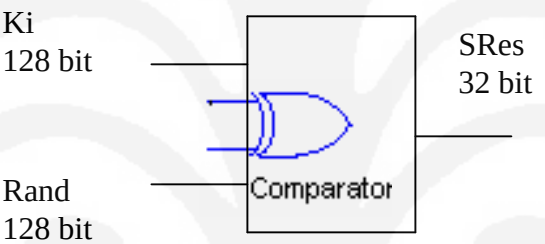
1. Keypad merupakan bagian dari I/O yang mengirimkan sinyal pin ke port PPI 82C55 dan membutuhkan alamat dari mikrokontroller untuk mengoperasikannya. Alamat PPI 82C55 mulai dari 2000H-3FFFH di dalam mikrokontroller.
2. Mikrokontroller melakukan pengiriman data terhadap LCD sebagai output penampil, dan LCD mengolah masukan apa saja dari setiap perintah eksekusi yang ingin ditampilkan dari mikrokontroller.
3. Proses eksekusi dapat juga ditampilkan di layar monitor menggunakan layar hyper terminal.

3. 3 PERANCANGAN SOFTWARE

Dalam suatu blok sistem perancangan software, dibutuhkan alat yang berfungsi sebagai pengolah data, yang mengambil data dan mengirimkan data kembali. Oleh karena itu maka digunakanlah Mikrokontroller AT89S52 sebagai *interface* indikator sistem informasi yang menghasilkan data Ki dan SRes (*Sinyal Respon*), yang memiliki input:

1. Input dari keypad jika, simulasikan nilai Ki yang tersimpan maupun nilai Rand. Input keypad juga sebagai pembuka pasword dan menjalankan instruksi selanjutnya.
2. Hasil input tersebut akan diolah dengan algoritma A3 dalam mikrokontroller AT89S52 yang kemudian akan mengirimkan data tersebut pada masukan perangkat output berupa LCD.
3. Proses komputasi/perhitungan dalam algoritma A3 akan menghasilkan keluaran simulasi yang terdiri dari sinyal respon (SRes) dengan ukuran sebesar 32 bit.

Perancangan algoritma A3 dapat direpresentasikan pada Gambar 3.3 berupa:



Gambar 3.3 Desain Algoritma A3.

Penjelasan desain algoritma dari Gambar 3.3 sebagai berikut:

1. Masukan simulasi berupa bilangan acak (Rand) dengan ukuran sebesar maksimal 128 bit dan kunci autentikasi (Ki) dengan ukuran sebesar maksimal 128 bit akan di kompresi datanya menjadi 64 bit dari Rand dan 64 bit dari Ki.
2. Kedua masukan yang telah di kompresi kemudian xor kan, agar berfungsi sebagai komparator, bertujuan untuk menghindari/mencegah kemungkinan timbulnya hasil keluaran komputasi yang identik.

Algoritma A3 (*Algorithm Function for Authentication*) tersebut merupakan suatu *one–way function* dengan tingkat kerahasiaan/keamanan yang tinggi, yang mana beroperasi dengan aspek pemrosesan yang kompleks terhadap Rand dan Ki, sedangkan proses komputasi/perhitungan terhadap kedua parameter tersebut dilakukan secara sederhana :

A3 = (2 * Z[m] + Z [n]) mod 2 $^{(9-j)}$ [13].....(3.1)

Dimana :

Z[m] = Elemen dari Ki (*Individual Subscriber Authentication Key*) 128 bit

Z[n] = Elemen dari Rand (*Random Number*) 128 bit

j = Level kompresi data (Memiliki 5 level kompresi data)

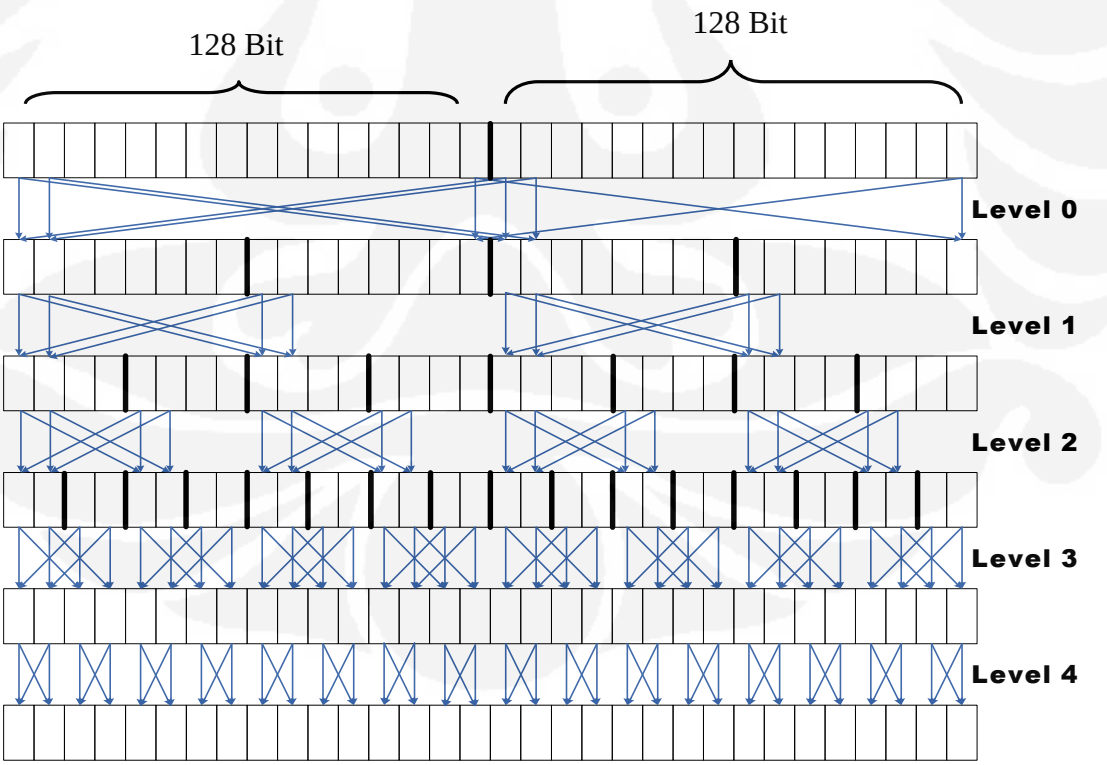
Rumusan Algoritma A3 merupakan bagian dari rumusan dari SRes

SRES = A3 [RAND, Ki] .....……(3.2)

Berdasarkan persamaan (3.2) serta desain algoritma A3 pada gambar 3.3, maka dapat diturunkan suatu rumusan sebagai berikut :

$$SRES = \overline{[(RAND_{compressed} \oplus Ki_{compressed})_{compressed}]} \quad \text{.....(3.3)}$$

Proses komputasi yang terjadi pada algoritma A3 dipermudah dengan cara adanya proses kompresis data dari kedua masukan dengan cara mengkompresi data dengan struktur kupu-kupu (*Butterfly Stukture)* [14] pada Gambar 3.4 dengan pola :



Gambar 3.4 Kompresi data dengan struktur kupu-kupu [12]

- Lima level kompresi
- Di setiap level kompresi pada Gambar 3.4 menghasilkan byte tergantung dari kedua masukan byte sebelumnya dengan rumusan :

$$X = (Z[m] + 2 * Z[n]) \bmod 2^{(9-j)} [13] \quad (3.4)$$

$$Y = (2 * Z[m] + Z[n]) \bmod 2^{(9-j)} [13] \quad (3.5)$$

$$Z[m] = T_j[X]$$

$$Z[n] = T_j[Y]$$

Dimana :

X = Elemen data baru sisi kiri

Y = Elemen data baru sisi kanan

Z [m] = Elemen dari Ki (*Individual Subscriber Authentication Key*) sebesar maksimal 128 bit

Z [n] = Elemen dari Rand (*Random Number*) sebesar maksimal 128 bit

j = Level kompresi data (Memiliki 5 level kompresi data)

- Kedua masukan byte digunakan untuk menentukan index dari *lookup table,* masukan *lookup table* akan digunakan untuk memperbaharui hasil byte
- *Lookup table* digunakan oleh level i sebagai table Ti dan berisi 2^{9-i} dari nilai 8-i bit, contohnya dapat diketahui pada table 3.1

Table 3.1 Hasil data kompresi menggunakan *Butterfly stukture*

Level	Nama Table	Jumlah Masukan	Nilai
1	T1	$2^9 = 512$	(9-i) Value = 8 bit
2	T2	$2^8 = 256$	(8-i) Value = 7 bit
3	T3	$2^7 = 128$	(7-i) Value = 6 bit
4	T4	$2^6 = 64$	(6-i) Value = 5 bit
5	T5	$2^5 = 32$	(5-i) Value = 4 bit

- *Pseudocode*:

- Load Rand ke dalam Z [16...31]

Data Rand yang berjumlah 32 byte di gabungkan dengan nilai data sebelahnya menjadi satu data array ke-j pada variable Z

Contoh:

Rand = 23553cbe9637a89d218ae64dae47bf35

23	55	3c	be	96	37	a8	9d	21	8a	e6	4d	ae	47	Bf	35

Nilai data tersebut di ubah ke desimal untuk ditempatkan dalam variable Y

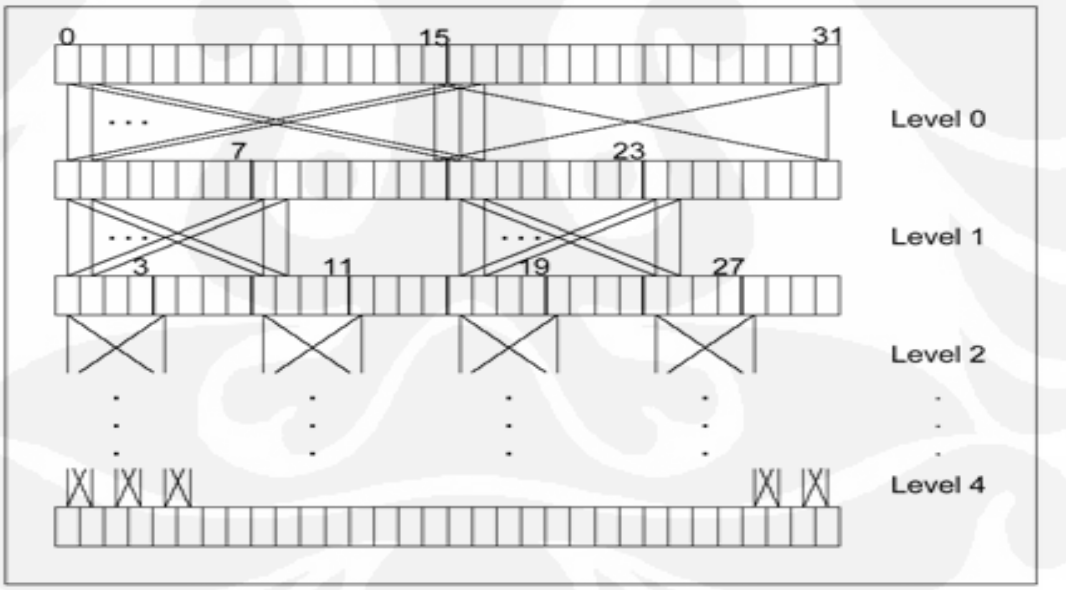
- Load Ki ke dalam Z [0..15]

Begitu pun dengan nilai Rand, Jumlah Ki yang berjumlah 32 byte di tempatkan di matrik Z [0...15] dengan cara dipasangkan dengan nilai sebelahnya kemudian harus di ubah ke desimal dengan pola yang sama dengan Nilai data Rand

Ki = 465b5ce8b199b49faa5f0a2ee238a6bc

46	5b	5c	e8	b1	99	b4	9f	aa	5f	0a	2e	e2	38	a6	Bc

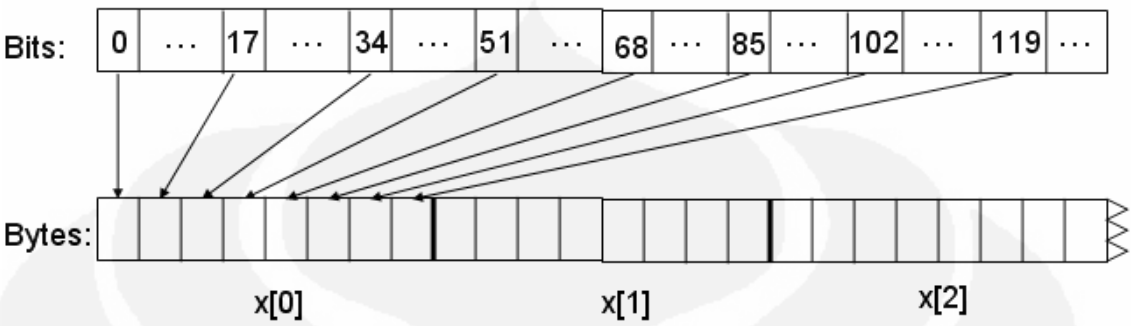
- Lakukan proses kompresi data Ki dan Rand seperti yang terlihat di Gambar 3.5



Gambar 3.5 Proses kompresi data dengan strukur kupu-kupu [12]

Proses komputasi dalam kompresi dilakukan dengan cara nilai data baru didapatkan dengan cara hasil komputasi data sebelumnya disubstitusikan dengan nilai data yang ada di table. Komputasi data dengan pola awal dengan cara proses komputasi elemen matrik Z [0] di komputasi dengan elemen matrik Z[16] begitu seterusnya. Tiap level dilakukan komputasi setengah level komputasi sebelumnya.

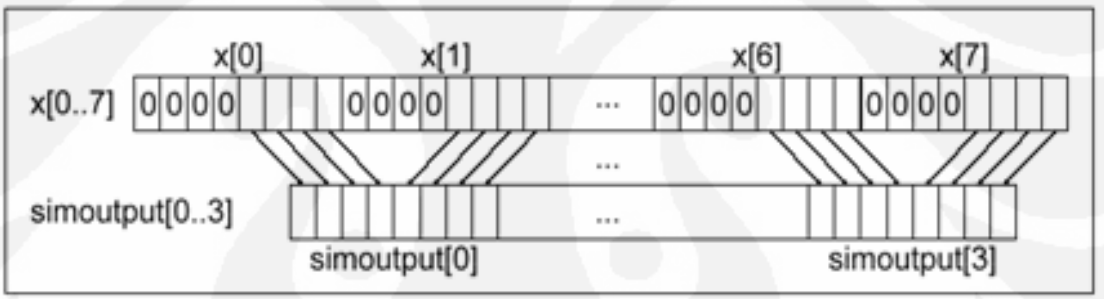
- Mengubah byte ke dalam bit
- Lakukan proses permutasi seperti terlihat di Gambar 3.6



Gambar 3.6 Proses pembentukan byte menjadi bit[12]

- Kompresi data output dari 16 byte menjadi 12 byte
- SRes pada Gambar 3.7 di peroleh 4 byte dari output 12 byte keluaran simcard

Proses pengambilan 4 byte SRes dengan cara pengambilan 4 bit dari elemen array sebelumnya (perubahan byte menjadi bit).



Gambar 3.7 Proses pengambilan nilai SRes dengan cara permutasi[12]

3.3.1 Kompresi data dengan stuktur kupu-kupu (b*utterfly stukture)*

Pada desain algoritma A3 dilakukan proses kompresi terhadap data masukan simulasi (Ki dan Rand) dengan menggunakan Kompresi yang menerapkan metode yang menyerupai struktur kupu-kupu (*Butterfly strukture*). Pada dasarnya kompresi ini meliputi pembacaaan suatu deretan nilai Ki dan Nilai Rand dalam desimal yang disusun menjadi satu matrik.

Nilai-Nilai input Ki dan Rand yang dimulai dengan masukan simulasi dari keypad berupa hexa desimal di konversi dulu ke dalam desimal agar proses kompresi data dengan struktur kupu-kupu bekerja. Nilai Ki dan Rand yang telah di konversi ke

desimal tersebut di tempatkan dalam 2 elemen yaitu elemen X (di posisi MSB) dan elemen Y (di posisi LSB) kedua elemen tersebut ditempatkan dalam satu matrik yaitu matrik Z, maka matrik Z = [X,Y], Elemen X adalah nilai Ki yang ditempatkan pada matrik Z di posisi array ke [1...15] sedangkan Elemen Y adalah nilai Rand yang ditempatkan pada matrik Z di posisi array ke [16...31], maka matrik Z yang terdiri dari masukan Ki dan Rand sebesar 32 byte.

Input Ki = 465b5ce8b199b49faa5f0a2ee238a6bc

Ubah ke desimal:

70	91	92	232	177	153	180	159	170	95	10	46	226	56	166	188

Input Rand = 23553cbe9637a8218ae64dae47bf35

Ubah ke desimal:

35	85	60	190	150	55	168	157	33	138	230	77	174	71	191	53

Nilai desimal pertama di tempatkan di level pertama kompresi data struktur kupu-kupu menjadi acuan untuk mendapatkan nilai level ke-n dari X-n dan Y-n dengan urutan perkalian silang antara Ki dan Rand dengan pola:

$Xn = (X[n] + 2 * Y[n]) \bmod 2^{(9-j)}[12]$ .....(3.4)

$Yn = (2 * X[n] + Y[n]) \bmod 2^{(9-j)}[12]$ .....(3.5)

Z [n] = T j [Xn]

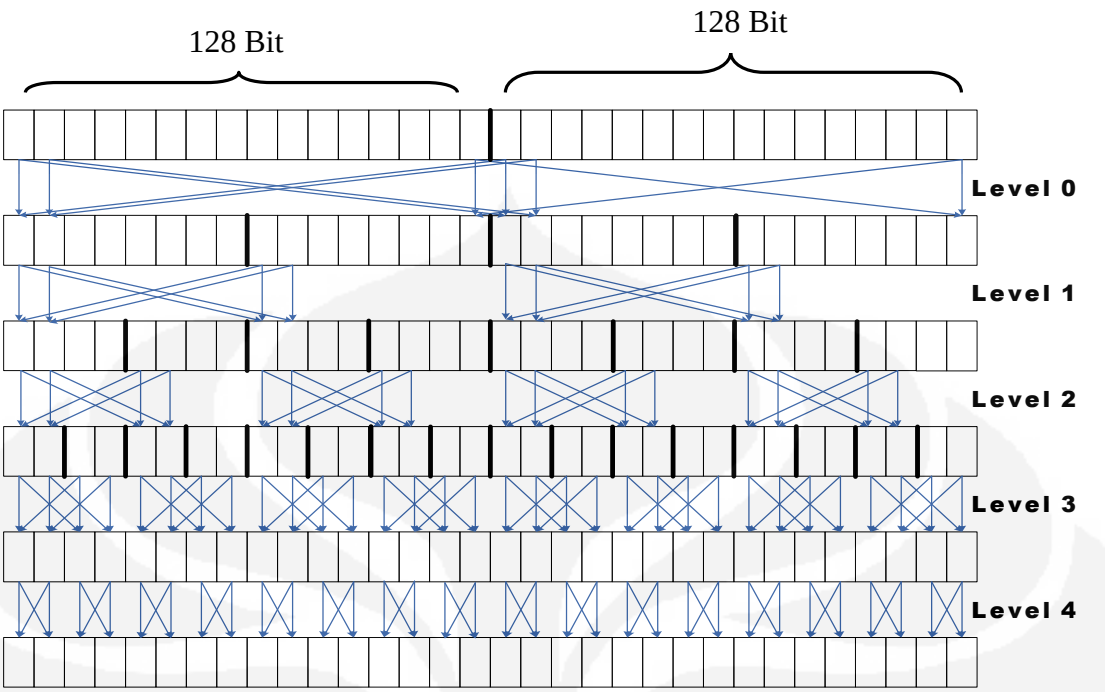
Z [n] = T j [Yn]

Dimana:

Xn = Elemen X di level ke-n

Yn = Elemen Y di level ke-n

Z[n] = Matrik Z berisi nilai baru setelah X ke-n dan Y ke-n di dapat dari hasil komputasi sebelumnya di substitusikan dengan nilai yang ada pada tabel autentikasi. Gambar 3.4 menjelaskan secara gambar pola kondisi komputasi kompresi dengan kupu-kupu.



Gambar 3.8 Kompresi data dengan struktur kupu-kupu [12]

Pola komputasi pada Gambar 3.8

1. level pertama melakukan komputasi dimulai dengan langkah dari array matrik Z[0] dengan array matrik Z[16] dan seterusnya, sehingga nilai data yang terdapat pada matrik Z di level pertama sebesar 8 bit.

Proses: Ambil Z ke [0] dan Z ke [16]

X = (Z [0] + 2* Z [16]) Mod 512

Y = (2* Z [0] + Z [16]) Mod 512; dimana T1 untuk level 1

Z [0] = T1 [X]; Hasil X di substitusikan dengan table 512

Z [16] = T1 [Y]; Hasil Y lookup table dengan table 512

Lakukan proses ini hingga Z ke 15 (dari elemen Ki) dan Z ke [31] (dari elemen Rand)

2. Untuk level kedua komputasi kompresi dilakukan dengan langkah setengah dari langkah dari komputasi pertama dari array matrik Z, maka level kedua dimulai dari array matrik Z[0] dengan array matrik Z[9] dan seterusnya, kemudian di substitusikan hasilnya ke tabel autentikasi untuk mendapatkan data baru. nilai data yang terdapat pada matrik Z di level kedua sebesar 7 bit hasil dari proses komputasi silang dan substitusi dari level sebelumnya.

Proses: Ambil Z ke [0] dan Z ke [9]

X = (Z [0] + 2* Z [9]) Mod 256

X = (2* [0] + Z [9]) Mod 256; dimana T2 untuk level 2

Z [0] = T2 [Y]; Hasil Y di substitusikan dengan table 256

Z [9] = T2 [X]; Hasil Z lookup table dengan table 256

Lakukan proses ini hingga Z ke 31

3. Untuk level ketiga komputasi kompresi dilakukan dengan langkah setengah dari langkah dari komputasi kedua dari array matrik Z, maka level ketiga dimulai dari array matrik Z[0] dengan array matrik Z[5] dan seterusnya, kemudian di substitusikan hasilnya ke tabel autentikasi untuk mendapatkan data baru. nilai data yang terdapat pada matrik Z di level ketiga sebesar 6 bit hasil dari proses komputasi silang dan substitusi dari level sebelumnya.

Proses: Ambil Z ke [0] dan Z ke [5]

X = (Z [0] + 2* Z [5]) Mod 128

X = (2* [0] + Z [5]) Mod 128; dimana T3 untuk level 3

Z [0] = T3 [Y]; Hasil Y di substitusikan dengan table 128

Z [5] = T3 [X]; Hasil Z lookup table dengan table 128

Lakukan proses ini hingga Z ke [31]

4. Untuk level keempat komputasi kompresi dilakukan dengan langkah setengah dari langkah dari komputasi ketiga dari array matrik Z, maka level keempat dimulai dari array matrik Z[0] dengan array matrik Z[3] dan seterusnya, kemudian di substitusikan hasilnya ke tabel autentikasi untuk mendapatkan data baru. nilai data yang terdapat pada matrik Z di level keempat sebesar 5 bit hasil dari proses komputasi silang dan substitusi dari level sebelumnya.

Proses: Ambil Z ke [0] dan Z ke [3]

X = (Z [0] + 2* Z [3]) Mod 64

X = (2* [0] + Z [3]) Mod 64; dimana T4 untuk level 4

Z [0] = T4 [Y]; Hasil Y di substitusikan dengan table 64

Z [3] = T4 [X]; Hasil Z lookup table dengan table 64

Lakukan proses ini hingga Z ke [31]

5. Untuk level kedua komputasi kompresi dilakukan dengan langkah setengah dari langkah dari komputasi keempat dari array matrik Z, maka level kelima dimulai dari array matrik Z[0] dengan array matrik Z[2] dan seterusnya, kemudian di substitusikan hasilnya ke tabel autentikasi untuk mendapatkan data baru. nilai data yang terdapat pada matrik Z di level kedua sebesar 4 bit hasil dari proses komputasi silang dan substitusi dari level sebelumnya.

Proses: Ambil Z ke [0] dan Z ke [5]

X = (Z [0] + 2* Z [2]) Mod 128

X = (2* [0] + Z [2]) Mod 128; dimana T3 untuk level 3

Z [0] = T3 [Y]; Hasil Y di substitusikan dengan table 128

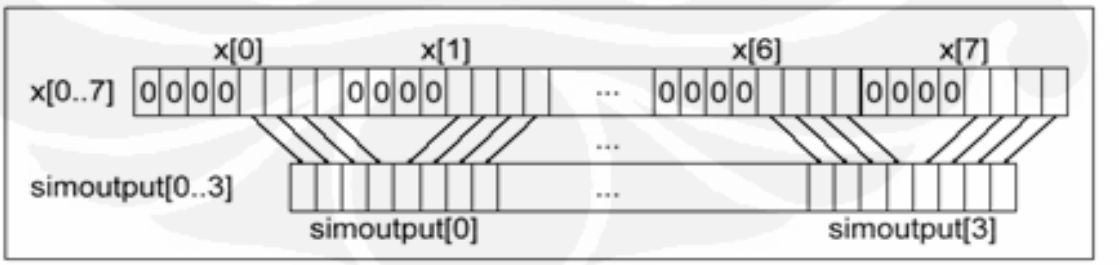
Z [2] = T3 [X]; Hasil Z lookup table dengan table 128

Lakukan proses ini hingga Z ke 31

Inti dari proses kompresi dengan struktur kupu-kupu adalah nilai data yang terdapat pada level berikutnya adalah hasil komputasi level sebelumnya di substitusikan dengan nilai yang ada pada tabel autentikasi.

3.3.2 Permutasi Data

Permutasi adalah salah satu langkah untuk mendapatkan matrik-matrik baru untuk mendapatkan nilai SRes. Nilai SRes merupakan hasil permutasi dari elemen yang di hasilkan dari nilai terakhir dari proses kompresi data ke lima yang di ubah dalam bit. Permutasi dilakukan dengan cara pengambilan data 4 bit terakhir dari matrik sebelumnya.



Gambar 3.9 Komputasi data untuk menghasilkan nilai SRes [12]

Elemen dari matrik-matrik yang sebelumnya hasil pembentukan dari perubahan byte ke bit, ditunjukkan pada Gambar 3.9 diambil 4 bit terakhir (*per nibble*) untuk di susun menjadi matrik-matrik baru untuk menjadi nilai SRes

Modifikasi Algoritma A3 yang dibuat dengan algoritma yang telah ada sebelumnya terdapat perbedaan pada proses kompresi data, proses kompresi data yang ada sebelumnya menerapkan proses kompresi menggunakan metode *adaptive Hufman coding* yang menerapkan proses pembacaan suatu deretan simbol/karakter, kemudian merubahnya ke dalam suatu bentuk kode-kode tertentu berdasarkan model, yang mana merupakan suatu kumpulan data statistik serta pola aturan yang digunakan untuk memproses simbol-simbol tersebut.

Konsep dasar dari kompresi data dengan metode struktur kupu-kupu adalah dengan membuat matrik-matrik baru dengan nilai data semakin kecil nilai bitnya dari matrik sebelumnya dengan proses kompresi lima level.

Keuntungan metode kompresi dengan struktur kupu-kupu, diakhir dari proses kompresi menghasilkan keluaran nilai data sebesar 32 bit (*output* SRes) sehingga tidak diperlukan proses kompresi tahap dua sehingga algoritma A3 yang dijalankan lebih efektif.

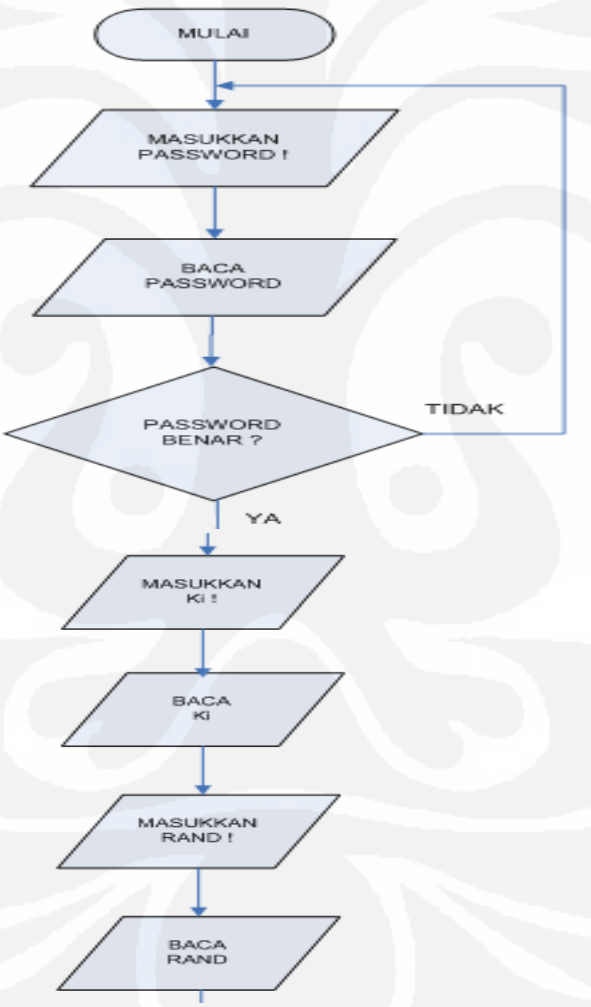
3.4. ALGORITMA SISTEM AUTENTIKASI

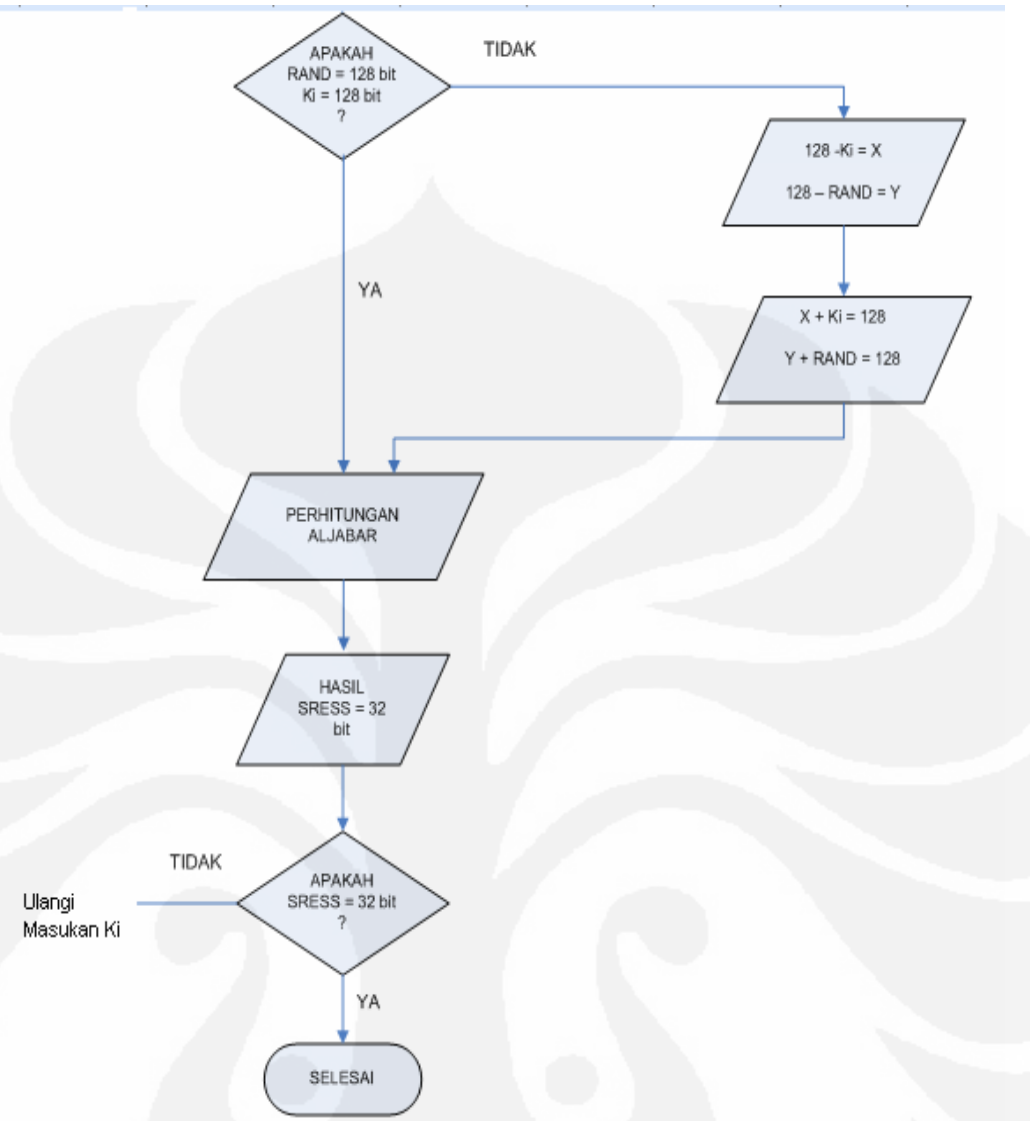
Algoritma program pengolahan data mikrokontroller akan diproses sebagai berikut:

1. Langkah awal algoritma pada perancangan sistem ini adalah: program akan menunggu masukan password dari keypad, jika password salah maka program akan looping kembali untuk menunggu masukan password yang benar.
2. Jika masukan password yang diinginkan program benar, maka selanjutnya adalah program akan menunggu masukan data dari simcard reader secara serial.
3. Setelah itu simulasi dapat dilakukan menggunakan masukan simulasi. Mikrokontroller dengan menunggu input simulasi pada keypad dari tombol 1_{hexa} sampai F_{hexa},
4. Masukan dari keypad berupa data Ki (*Individual Subscriber Authentication Key*) sebesar maksimal 128 bit biner akan di ubah kedalam nilai hexa desimal.

5. Apabila nilai Ki dan Rand kurang dari 128 bit maka algoritma akan melakukan proses penambahan input agar diperoleh output sesuai yang diharapkan.
6. Nilai Ki (*Individual Subscriber Authentication Key*) kemudian di komputasi dengan nilai dari sinyal acak (Rand) yang telah di bangkitkan di mikrokontroller.
7. Program melakukan proses komputasi kedua masukan
8. Hasil komputasi tersebut akan menghasilkan sinyal respon yang menyatakan proses authentikasi simcard GSM telah berhasil.

3.5 FLOWCHART SISTEM AUTENTIKASI





Gambar 3. 10 Flowchart sistem autentikasi simcard GSM

Penjelasan dari flowchart dari gambar 3.10 sebagai berikut:

1. Langkah awal perancangan sistem ini adalah dengan menentukan port- port yang akan difungsikan untuk I/O pada sistem ini.
2. Inisialisasi keypad yang akan difungsikan sebagai input password dan simulasi masukan data Ki. (PA.0 – PA.2 sebagai port output dan PB.0 – PB.3 sebagai input pada pembacaan keypad matriks 4 x 4).
3. Masukan password pembuka agar hanya pelanggan yang berhak yang bisa mengakses
4. Masukan password dengan benar, jika benar akan terbuka jika salah lakukan kembali masukan password.

5. Simulasi masukan Ki melalui keypad 4x4 sebesar 16 byte
6. Simulasi Masukan Rand sebesar 16 byte.
7. Kedua masukan Ki dan Rand harus berjumlah 128 bit, apabila kurang dari 128 bit, algoritma akan melakukan proses penambahan masukan.
8. Mikrokontroller menjalankan algoritma A3 dengan mengkomputasi kedua masukan Ki dan Rand sehingga menghasilkan SRES
9. Nilai SRes terbaca penuh di layar LCD.
10. Jika SRes belum terbaca di LCD ulangi lagi proses masukan data Ki dengan masukan simcard reader atau melalui masukan keypad.
11. Pengulangan masukan data Ki dapat di lakukan dari 2 input yang ada melalui keypad.
12. Proses berakhir dengan menampilnya data SRes di LCD sebesar 32 bit, apabila kurang dari 32 bit lakukan proses pengulangan input Ki dan Rand sehingga mendapatkan nilai SRes yang benar.

BAB 4
PERANCANGAN HARDWARE

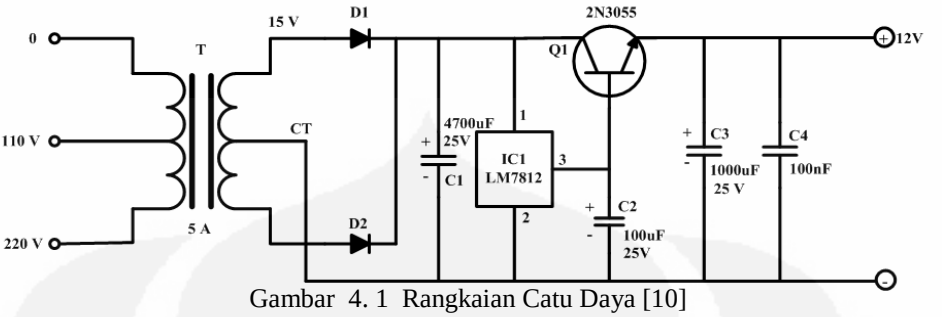
Sistem perangkat keras *(hardware)* pada sistem ini dapat dibagi menjadi 3 bagian, yaitu bagian sistem pengolah informasi, bagian sistem simulasi, dan bagian sistem penampil *(display).* Masing-masing bagian sistem tersebut terdapat beberapa komponen pendukung dimana komponen pendukung tersebut mempunyai fungsi menurut bagiannya sendiri-sendiri.

4.1 RANGKAIAN CATU DAYA

Kestabilan tegangan output dari power supply ini sangat penting mengingat modul ini menggunakan mikokontroler AT89S52 serta PPI 8255 yang sangat sensitif terhadap perubahan dari tegangan. Untuk itu hal utama yang harus diperhatikan adalah perancangan sebuah sistem catu daya (*power supply*) yang dapat bekerja dengan baik sehingga memiliki kestabilan output tegangan yang benar-benar baik dan memiliki ketahanan waktu pemakaiannya.

Power Supply pada Gambar 4.1 untuk sistem kerja alat menggunakan trafo CT 1 Ampere, sebagai pengaman maka pada power supply ini dipasang fuse, sehingga apabila ada masalah pada sistem maka akan otomatis memutuskan supply untuk mencegah kerusakan yang semakin parah.

Power supply ini memiliki tegangan output regulator 12VDC dan 9 VAC. 12 VDC digunakan untuk memberikan supply tegangan pada kipas sebagai pendingin untuk sistem tersebut, sedangkan 9 VAC digunakan untuk supply pada minimum sistem DT-51, karena pada modul DT-51 sudah memiliki sistem catu yang mengubah 9 VAC menjadi regulator 5 volt sehingga tegangan pada modul tersebut menjadi stabil walau tegangan inputnya naik turun.



Gambar 4. 1 Rangkaian Catu Daya [10]

4. 2 MINIMUM SISTEM DT-51

Rangkaian mikrokontroller merupakan pusat pengolahan data dan basis dari informasi data. Dimana Mikrokontroller yang digunakan pada modul minimum sistem DT-51 Ver. 3. 3, menggunakan mikrokontroller tipe AT89S52. Pada modul ini juga terdapat eksternal RAM dengan kapasitas memory 64 Kbyte (28HC64) dan PPI 8255 (*Programmable Peripheral Interface*). Pada PPI 8255 ini memiliki 4 *Port* Utama sebagai *interface* data bus. Ke-empat *port* tersebut adalah:

1. *Port* A, port ini digunakan sebagai *output* (*address* 2000H)
2. *Port* B, port ini digunakan sebagai *input* (*address* 2001H)
3. *Port* C dan *Port* 1 digunakan sebagai *output* (*address* 2002H)
4. *Port Control Word Register* (2003H)

Dapat dijelaskan sebagai berikut :

1. *Port* A, *port* ini digunakan sebagai *output* (*address* 2000H)

   Out &H2000 , A1

   A1 merupakan *register* yang digunakan untuk mengeluarkan aplikasi pada *keypad*. Penggunaan *address* 2000H untuk mengaktifkan *port* A sebagai *output* pada *keypad* matriks 3x4, sehingga *keypad* tersebut dapat berfungsi sebagai *output* kolom data untuk masukan data simulasi.

2. *Port* B, *port* ini digunakan sebagai *input* (*address* 2001H)

   B1 = Inp(&H2001)

   B1 merupakan *register* yang digunakan untuk memberikan masukan aplikasi pada *keypad*. Penggunaan *address* 2001H adalah untuk mengecek bit data pada *port* B

sebagai *input* tombol dari *keypad* matriks 3x4, sehingga *keypad* tersebut dapat mampu membaca baris data pada *keypad*.

3. *Port* C dan *Port* 1 digunakan sebagai *output* (*address* 2002H)

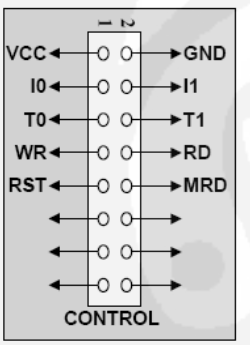
   Penggunaan *port* C ini untuk mengeluarkan semua simulasi sensor dari *keypad* matriks 3x4 jika ada penambahan *output* simulasi berupa buzzer atau led.

4. *Port Control Word Register* (2003H)

   Fungsi *port* ini untuk mengaktifkan *keypad* pada posisi Write, sehingga *keypad* bisa difungsikan sebagai *input*.

   Misal : **Out &H2003 , &B10000010**

   Ini berarti 8 bit yang difungsikan yaitu 10000010 bit referensi untuk mengaktifkan fungsi *port* pada kondisi ’write’. Bit ke -7 merupakan bit control untuk kondisi ‘write’. Dimana diagram *port control* dapat dilihat pada Gambar 4.2.



Gambar 4.2 Diagram *port control* [11]

Selain memiliki PPI 8255 (*programmable Peripheral Interface*), modul DT-51 juga memiliki RAM eksternal 28HC64, sehingga untuk penyimpanan data, selain bisa disimpan pada memory internal (0000H – 1FFFH) juga dapat disimpan pada memory eksternal (6000H – FFFFH). Dengan adanya memory eksternal ini maka dapat memudahkan penyimpanan data sementara *(temporary data storage)* pada pemrograman BASCOM IDE 8051. Penyimpanan data sementara dapat berupa data bit, byte, word, dan integer. Ukuran dari data tersebut adalah, bit memiliki ukuran data 0 dan 1, byte memiliki ukuran data 0 – 255, word memiliki ukuran data 0- 2047, integer memiliki ukuran data -32767 - +32768.

Pada perancangan sistem ini eksternal RAM digunakan untuk menyimpan akuisisi data (database) untuk simulasi sensor dengan tombol *keypad*. Selain itu juga eksternal RAM digunakan untuk menyimpan data yang sudah *fixed* untuk nilai pembacaan sensor. Data pada eksternal RAM tersebut akan tersimpan terus sampai data tersebut dihapus/ ditumpuk dengan data yang lain. Data yang tersimpan pada eksternal RAM ini bisa berupa byte, string, integer maupun word. Sistem ini menyimpan data pada eksternal RAM dengan type data word. Untuk dapat menyimpan data pada eksternal RAM maka harus ditentukan dulu penamaan untuk alamatnya. Pada pemrograman BASCOM IDE 8051 program akan otomatis menyimpan data ke eksternal RAM hanya dengan mengakses nama untuk alamat eksternal tersebut, misalnya :

```
DIM LSAVE_DATA AS XRAM  BYTE
LSAVE_DATA = 100
```

Dengan menggunakan instruksi diatas maka data 100 akan tersimpan secara otomatis ke dalam LSAVE_DATA pada eksternal RAM. Sehingga untuk mengakses data tersebut hanya dengan menginisalisasikan nama *address*nya saja yaitu LSAVE_DATA.

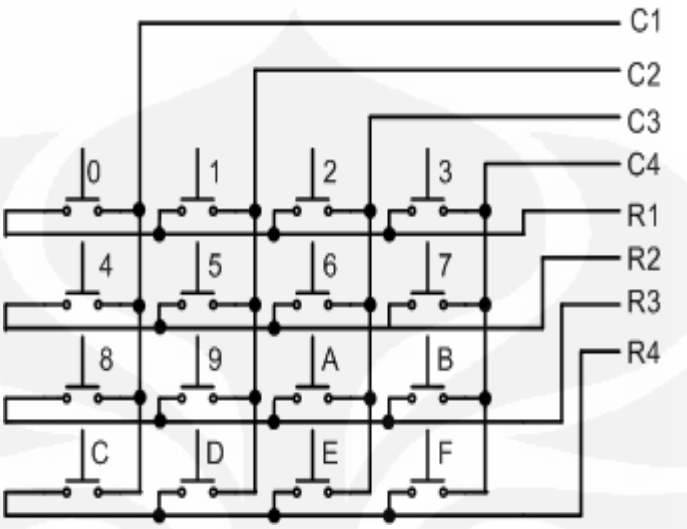
4. 3 PERANGKAT *INPUT* SIMULASI

Perangkat input simulasi terdiri dari beberapa perangkat pendukung, yang bertujuan memberikan masukan berupa data Ki (*Individual Subscriber Authentication Key*) ke program pengolah. Adapun perangkat pendukung tersebut terdiri atas keypad.

4.3.1 KEYPAD

Keypad yang digunakan pada system ini adalah keypad matriks 4x4 yang terlihat pada Gambar 4.4. Keypad pada sistem ini memiliki fungsi sebagai input data password dan input data untuk simulasi sensor. Perancangan program keypad untuk simulasi ini adalah dengan metode ’grounding’, maksudnya adalah bit akan dalam kondisi ’0’ ketika tombol keypad tersebut ditekan. Hal ini dilakukan karena pin-pin dari port PPI sudah dalam kondisi high atau kondisi ’1’ sebelumnya sehingga nilai

dari semua port pada PPI tersebut adalah 255 (FFH = 11111111). Sehiingga dengan menggunakan metode grounding akan memudahkan pengecekan bit-bitnya.



Gambar 4.3 Hubungan keypad 4X4 [12]

4.4 PERANGKAT *OUTPUT* SIMULASI

Perangkat output simulasi berfungsi menampilkan setiap hasil dari perubahan kondisi yang terjadi baik saat kondisi simulasi belum berjalan (masih dalam kondisi password belum dibuka) maupun kondisi simulasi telah dijalankan (SRes mampu ditampilkan). Perangkat penampil informasi yang lazim digunakan adalah LCD (*Liquid Crystal Display*)

4.4.1 LCD (*Liquid Crystal Display*)

Pada perancangan untuk alat ini, LCD (*Liquid Crystal Display*) yang digunakan adalah LCD dengan ukuran 2x16 .Untuk dapat menghasilkan fungsinya sebagai penampil (*display*) pada alat ini, maka sebelumnya harus disesuaikan dulu konfigurasi dari pin-pinnya. Semua pin-pin dari LCD (*Liquid Crystal Display*) tersebut harus terkoneksi dengan tepat pada modul DT-51. Kemudahan dari Modul

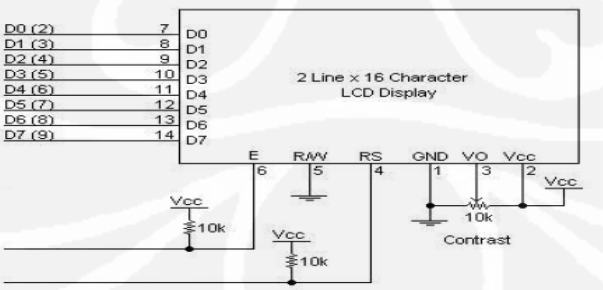
ini adalah telah disediakannya port khusus untuk semua pin dari LCD, sehingga hal ini mampu mengurangi kesalahan dalam pemasangan pin-pin dari LCD. Setelah pemasangan semua pin-pin tersebut telah selesai,maka dilakukan adjusment terhadap intensitas dari lampu dan kursor pada LCD, sehingga mampu menampilkan karakter yang dapat terlihat dengan jelas.

Pada sistem ini LCD (*Liquid Crystal Display*) difungsikan sebagai *output* untuk menampilkan semua instruksi-instruksi dan informasi yang berkaitan dengan sistem kerja alat ini, sehingga dengan adanya LCD ini tidak terjadinya kesalahan prosedur dalam pengaplikasiannya. Hal-hal yang berkaitan dengan fungsi kerja dari LCD ini antara lain:

- Menampilkan semua input dari keypad baik berupa data password maupun berupa data input simulasi.
- Menampilkan informasi berupa status proses pencarian nilai triplet-triplet autentikasi.
- Menampilkan proses komputasi dan output proses komputasi.

Adapun fitur yang disajikan dalam LCD ini adalah:

a. Terdiri dari 16 karakter dan 2 baris
b. Mempunyai 192 karakter tersimpan
c. Terdapat karakter generator terprogram
d. Dapat dialamati dengan mode 8-bit dan 4-bit
e. Dilengkapi dengan *backlight*



Gambar 4.4 LCD 16x2 [13]

Pada Gambar 2.9 LCD ini terdiri dari 8 jalur data, 3 jalur kendali dan fasilitas pengaturan kontras serta *backligh*t. LCD ini dapat dikendalikan dengan mikrokontroller atau mikroposesor.

Deskripsi fungsi-fungsi pin dari penampil LCD (*Liquid Crystal Display*) ini adalah:

1. VSS, sebagai suplai 0 volt atau ground.
2. VDD, sebagai suplai input untuk LCD (5 volt).
3. VO, sebagai tegangan operasi untuk LCD atau pengaturan kontras layer.
4. RS, sebagai jalur data dan penghantar kode instruksi. (H: DATA, L: kode instruksi.
5. R/W, sebagai jalur baca-tulis data ke mikroprosesor.
6. E, sebagai sinyal *enable* bagi *chip*.
7. DB0-DB7, sebagai data bit 0 sampai dengan data bit 7.

4.5 RS – 232

Pada modul DT-51 terdapat port serial yang dapat di interkoneksikan dengan *interface* apapun secara serial. Sistem ini menggunakan RS-232 untuk diaplikasikan dalam komunikasi data secara serial dengan personal komputer. Koneksi antara personal komputer dan modul DT-51 dengan menggunakan kabel data yang dihubungkan dengan kabel serial (*male to male DB-9*) yang selanjutnya *output* dari kabel serial tersebut dihubungkan ke port serial DT-51, sehingga segala eksekusi yang sedang dilakukan oleh mikrokontroller dapat terbaca oleh personal komputer.

Pada pin RS-232 ini terdapat pin Rx dan Tx, pin-pin inilah yang bekerja menghasilkan sinyal-sinyal berupa data ketika terjadi interkoneksi secara serial antara mikrokontroller dengan interface lain.

BAB 5

UJI COBA DAN ANALISIS

5.1 PROSEDUR SIMULASI

Uji coba simulasi dilakukan untuk menganalisis karakteristik unjuk kerja dari rancangan algoritma A3 serta proses autentikasi. Uji coba simulasi ini terdiri dari dua bagian uji karakteristik unjuk kerja yaitu :

- Uji karakteristik unjuk kerja algoritma A3
- Uji karakteristik unjuk kerja proses autentikasi terhadap usaha pemalsuan Ki.

Struktur perangkat model simulasi terdiri dari mokrokontroller AT9S52, dimana mikrokontroller berfungsi sebagai pengsimulasi penghitung data autentikasi pada sisi pelanggan

Langkah pertama yang harus dilakukan adalah menentukan nilai Ki (yang di simulasikan dengan masukan dari keypad) sebesar maksimal 16 byte apabila kurang dari 16 byte algoritma tidak bisa melakukan proses simulasi komputasi ke langkah berikutnya. Sesaat setelah akses dilakukan, proses autentikasi segera dilaksanakan. Saat itu, seiring dengan dibangkitnya triplet-triplet autentikasi yang dialokasikan untuk MS tersebut, maka segera diproses dengan algoritma A3 sehingga pada akhir proses komputasi akan dihasilkan SRes (sebesar maksimal 32 bit). Kemudian algoritma akan memeriksa apakah SRes tersebut telah mempunyai data sampai 32 bit jika kurang dari ketentuan maka algoritma akan mengulang proses masukan data Ki dan Rand,

Perubahan nilai Ki maupun Rand mempengaruhi nilai dari SRes tersebut,. Pengolahan Algoritma A3 dijalankan dengan tiga tahapan;

1. Mengkompresi kedua masukan dengan proses kompresi dengan lima level sehingga diharapkan nilai level terakhir menghasilkan nilai bit terkecil dari level-level sebelumnya.

2. Tahap kedua algoritma menjalankan proses pembentukan matrik untuk permutasi dari hasil perubahan byte menjadi bit dari hasil kompresi nilai data level lima menjadi nila bit.
3. Tahap Ketiga bit-bit yang dihasilkan dari nilai data level lima akan membentuk matrik-matrik baru untuk dilakukan proses permutasi, sehingga matrik-matrik yang di permutasi akan menghasilkan nilai SRes.

Komputasi akan dilakukan apabila algoritma kedua masukan Ki sebesar 128 bit dan Rand 128 bit, karena perhitungan mencari SRes menggunakan aljabar input nilai maksimal 128 bit

5.2 HASIL UJI COBA SIMULASI

5.2.1 Karakteristik Unjuk Kerja Algoritma A3

Uji coba karakteristik unjuk kerja dari rancangan algoritma A3 dilakukan untuk mengetahui jumlah kapasitas keluaran yang digunakan dari kedua masukan.

Untuk itu, maka uji coba dilakukan dengan menggunakan beberapa Ki dan Rand yang berbeda nilainya satu sama lain.

Berikut uji coba A, pengujian unjuk kerja algoritma A3:

A. Unjuk kerja algoritma A3 berdasarkan perhitungan secara manual.

Ki =

46	5b	5c	e8	b1	99	b4	9f	aa	5f	0a	2e	E2	38	a6	bc

Rand =

23	55	3c	be	96	37	a8	9d	21	8a	e6	4d	ae	47	bf	35

Dari kedua masukan tersebut diproses melalui beberapa tahapan, dimulai dengan proses kompresi terhadap nilai data dari kedua masukan

.

Hasil Kompresi

Nilai level 1 kompresi:

Variable X

70	91	92	232	177	153	180	159	170	95	10	46	226	56	166	188

Variable Y

35	85	60	190	150	55	168	157	33	138	230	77	174	71	191	53

Nilai level 5 kompresi:

Variable X

2	5	15	3	0	0	8	11	15	15	9	8	4	0	12	14

Variable Y

9	14	13	6	10	10	12	5	3	13	3	8	4	13	5	1

Proses pengolahan algoritma A3 berikutnya, tahap kedua dengan mengubah nilai data yang dihasilkan dari proses kompresi level lima kedalam nilai bit. Pembentukan bit dengan cara satu byte menghasilkan 4 bit (nibble)

Pengubahan byte dari hasil kompresi menjadi bit

0	0	1	0	0	1	0	1	1	1	1	1	0	0	1	1
0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1
1	1	1	1	1	1	1	1	1	0	0	1	1	0	0	0
0	1	0	0	0	0	0	0	1	1	0	0	1	1	1	0
1	0	0	1	1	1	1	0	1	1	0	1	0	1	1	0
1	0	1	0	1	0	1	0	1	1	0	0	0	1	0	1
0	0	1	1	1	1	0	1	0	0	1	1	1	0	0	0
0	1	0	0	1	1	0	1	0	1	0	1	0	0	0	1

Proses pengolahan algoritma A3 berikutnya, tahapan terakhir dengan melakukan permutasi dari matrik yang dibentuk dari pengubahan byte menjadi bit. Proses permutasi dilakukan dengan cara pengambilan 4 bit terakhir (LSB) dari matrik yang dibentuk dari pengubahan byte menjadi bit.

Permutasi

x	X	x	x	1	0	0	1	x	x	x	X	0	1	0	1
x	X	x	x	1	1	0	1	x	x	x	X	0	0	0	1
x	X	x	x	1	1	0	0	x	x	x	X	1	0	1	0
x	X	x	x	1	1	0	1	x	x	x	X	0	0	1	0

Ket :

x = diabaikan

SRes didapat dari proses permutasi dari matrik yang dibentuk dari pengubahan byte menjadi bit.

Jadi SRes

1	0	0	1	0	1	0	1	1	1	0	1	0	0	0	1
1	1	0	0	1	0	1	0	1	1	0	1	0	0	1	0

= 95D1CAD2

Untuk lebih jelasnya, akan dijelaskan disertai dengan rumus-rumus yang digunakan pada setiap tahapan dari pengolahan algoritma A3 tersebut.

Ki = [0...15] dan Rand = [16...31] diletakkan pada matrik kosong dengan format

Z = [0....31]

Proses dilakukan dengan:

Proses Kompresi

Level_1

Ambil Z ke m (0) dan Z ke n (16), Masukkan ke rumus

X = [Z (0) + 2* Z (16)] mod 512 [13].....(5.1)

Y = [2.* z (0) + z (16)] mod 512 [13].....(5.2)

Z[0] yang baru = T1 [X] look up tabel di tabel 512 ke-X

Z[16] yang baru = T1 [Y] look up tabel di tabel 512 ke-Y

X = untuk mencari elemen X [i] yang baru di sebelah kiri

Y = untuk mencari elemen Y [i] yang baru di sebelah kanan

Kompresi level 2 sampai dengan level 5 dilakukan dengan cara yang sama tetapi dengan modulus yang berbeda dan menggunakan look up tabel yang berbeda juga.

Hasil kompresi diproses kembali ke tahapan proses algoritma A3 berikutnya yaitu pengubahan byte menjadi nilai-nilai bit. Tiap byte diubah per nible atau 4 digit biner. Bit-bit tersebut disusun sebanyak 128 bit bertujuan untuk mendapatkan matrik untuk permutasi.

Proses pembentukan matrik untuk permutasi dari pembentukan bit dari nilai byte kompresi level terakhir

Mengubah hasil data kompresi terakhir dari byte menjadi bit terlebih dahulu

Diubah menjadi:

2	5	15	8	15

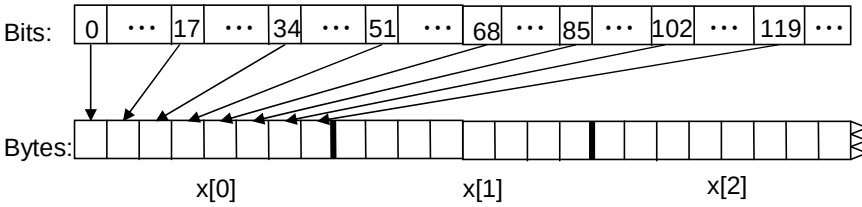
0010	0101	1111	1000	1111

Langkah berikutnya membuat matrik untuk permutasi berdasarkan pola pengambilan bit, dengan menggunakan rumus:

J = [8* x [j] + i] *17 mod 128 [13].....(5.3)

Matrik X = [0..31] dan Elemen i = [0..7] maka

Langkah pengambilan bit untuk mengisi matrik-matrik untuk permutasi X [j] dilakukan dengan cara:



Gambar 5.1 Proses pembentukan matrik untuk permutasi

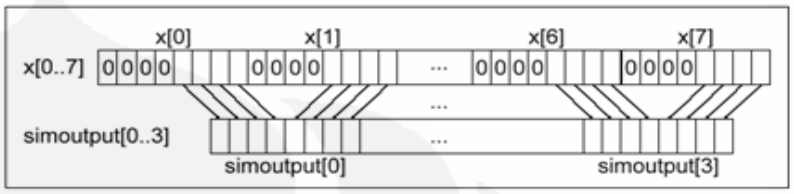
Angka-angka dibawah ini merupakan bit yang dihasilkan dari pengubahan byte menjasi bit dari hasil kompresi level lima. Nilai diatas dari bit biner tersebut untuk menandakan bit tersebut berada pada urutan bit yang keberapa bertujuan untuk mempermudah melakukan pengambilan bit sesuai dengan pola yang diinginkan untuk menjadi matrik untuk permutasi.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	1	0	0	1	0	1	1	1	1	1	0	0	1
16	17	18	19	20	21	22	23	24	25	26	27	18	29	30
0	0	0	0	0	0	0	0	1	0	0	0	1	0	1
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
1	1	1	1	1	1	1	1	1	0	0	1	1	0	0
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
0	1	0	0	0	0	0	0	1	1	0	0	1	1	1
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78
1	0	0	1	1	1	1	0	1	1	0	1	0	1	1
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94
1	0	1	0	1	0	1	0	1	1	0	0	0	1	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110
0	0	1	1	1	1	0	1	0	0	1	1	1	0	0
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126
0	1	0	0	1	1	0	1	0	1	0	1	0	0	0

				X[0]							X[1]			
x	x	x	x	1	0	0	1	x	x	x	x	0	1	0
				X[2]								X(3)		
x	x	x	x	1	1	0	1	x	x	x	x	0	0	0
				X(4)								X(5)		
x	x	x	x	1	1	0	0	x	x	x	x	1	0	1
				X(7)								X[7]		
x	x	x	x	1	1	0	1	x	x	x	x	0	0	1

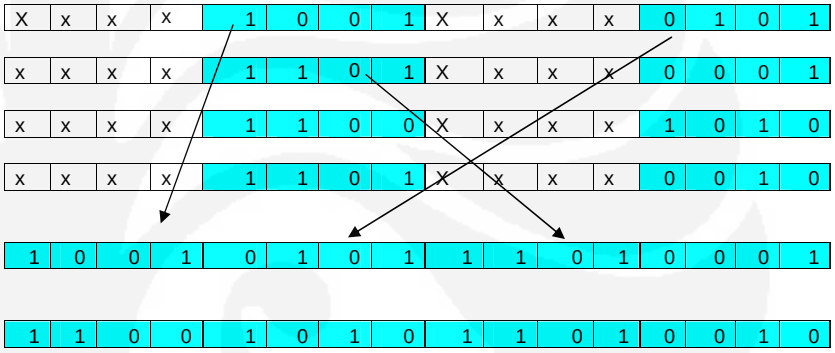
Angka yang berwarna biru merupakan langkah pengambilan bit untuk membuat matrik permutasi X[0], begitupun dengan langkah berikutnya untuk membuat matrik permutasi X[1] dan seterusnya.

4 bit terakhir dari matrik untuk permutasi pada Gambar 5.2 untuk membangkitkan nilai SRes pada Gambar 5.2 dengan cara permutasi dari matrik untuk permutasi:



Gambar 5.2 Pembentukan nilai keluaran (SRes) dari hasil permutasi [12]

Gambar 5.2 merupakan cara pembangkitan nilai SRes dengan permutasi diperoleh dari matrik untuk permutasi, diambil dari 4 bit terakhir dari tiap-tiap matrik untuk permutasi yang ditunjukkan pada Gambar 5.3 .



Gambar 5.3 Pengambilan bit yang dibutuhkan untuk membangkitkan SRes

Uji Coba B, Pengujian untuk pembuktian program telah bekerja sesuai algoritma A3

B. Unjuk kerja algoritma A3 menggunakan mikrokontroller pada sisi pelanggan

Input masukan melalui Keypad

Ki =

46	5b	5c	e8	b1	99	b4	9f	aa	5f	0a	2e	e2	38	a6	bc

Rand =

23	55	3c	be	96	37	a8	9d	21	8a	e6	4d	ae	47	bf	35

Simulasi masukan dengan menggunakan Keypad 4 x 4

Hasil Kompresi

Tabel 5.1 Variable X dari proses kompresi percobaan B

Variable X			
DT ARRAY X KE-1	**DT ARRAY X KE-15**	**DT ARRAY X KE-25**	**DT ARRAY X KE**
HSL KOMPRESI1=84	HSL KOMPRESI1=50	HSL KOMPRESI1=121	HSLKOMPRESI1=
IDX TABEL KE-67	IDX TABEL KE-217	IDX TABEL KE-127	IDX TABEL KE-1
HSL KOMPRESI2=96	HSL KOMPRESI2=91	HSL KOMPRESI2=75	HSL KOMPRESI2
IDX TABEL KE-67	IDX TABEL KE-217	IDX TABEL KE-127	IDX TABEL KE-1
HSL KOMPRESI3 =28	HSL KOMPRESI3 =46	HSL KOMPRESI3 =7	HSL KOMPRESI3
IDX TABEL KE-67	IDX TABEL KE-89	IDX TABEL KE-127	IDX TABEL KE-4
HSL KOMPRESI4 =6	HSL KOMPRESI4 =16	HSL KOMPRESI4 =19	HSL KOMPRESI4
HSL KOMPRESI5=4	HSL KOMPRESI5=6	HSL KOMPRESI5=12	HSL KOMPRESI5
IDX TABEL KE-3	IDX TABEL KE-25	IDX TABEL KE-31	IDX TABEL KE-1

Tabel 5.2 Variable Y dari proses kompresi percobaan B

Variable [Y]			
DT ARRAY Y KE-1	**DT ARRAY Y KE-15**	**DT ARRAY Y KE-25**	**DT ARRAY Y KE**
HSL KOMPRESI1=201	HSL KOMPRESI1=133	HSL KOMPRESI1=180	HSL KOMPRESI1=
IDX TABEL KE-84	IDX TABEL KE-213	IDX TABEL KE-136	IDX TABEL KE-20
HSL KOMPRESI2=111	HSL KOMPRESI2=105	HSL KOMPRESI2=44	HSL KOMPRESI2=
IDX TABEL KE-84	IDX TABEL KE-213	IDX TABEL KE-136	IDX TABEL KE-20
HSL KOMPRESI3=55	HSL KOMPRESI3=46	HSL KOMPRESI3=39	HSL KOMPRESI3=
IDX TABEL KE-84	IDX TABEL KE-85	IDX TABEL KE-8	IDX TABEL KE-20
HSL KOMPRESI4=4	HSL KOMPRESI4=27	HSL KOMPRESI4=17	HSL KOMPRESI4=
IDX TABEL KE-20	IDX TABEL KE-21	IDX TABEL KE-8	IDX TABEL KE-20
HSL KOMPRESI5=6	HSL KOMPRESI5=0	HSL KOMPRESI5=5	HSL KOMPRESI5=
IDX TABEL KE-20	IDX TABEL KE-21	IDX TABEL KE-8	IDX TABEL KE-20

Tabel 5.3 Hasil keluaran SRes (*Signal Response*) dalam biner percobaan B

Hasil SRes				
sresx[0]LSB:1	sresx[1]LSB:0	sresx[2]LSB:1	sresx[3]LSB:0	sresx[4]LSB:1
sresx[0]LSB:0	sresx[1]LSB:1	sresx[2]LSB:1	sresx[3]LSB:0	sresx[4]LSB:1
sresx[0]LSB:0	sresx[1]LSB:0	sresx[2]LSB:0	sresx[3]LSB:0	sresx[4]LSB:0
sresx[0]LSB:1	sresx[1]LSB:1	sresx[2]LSB:1	sresx[3]LSB:1	sresx[4]LSB:0
sresx[5]LSB:1	sresx[6]LSB:1	sresx[7]LSB:0		
sresx[5]LSB:0	sresx[6]LSB:1	sresx[7]LSB:0		
sresx[5]LSB:1	sresx[6]LSB:0	sresx[7]LSB:1		
sresx[5]LSB:0	sresx[6]LSB:1	sresx[7]LSB:0		

SRES = 95D1CAD2

Uji coba C, Pengujian untuk pembuktian program telah bekerja sesuai algoritma A3

C. Unjuk kerja algoritma A3 menggunakan mikrokontroller dengan masukan Ki dan Rand berbeda untuk mengetahui pengaruh keluaran yang dihasilkan sebagai referensi analisis.

Input melalui keypad

Ki =	fe	c8	6b	a6	eb	70	7e	d0	89	5	75	7b	1b	b4	4b	8f
Rand =	9f	7c	8d	2	1a	bc	f4	db	21	3c	cf	f0	c7	f7	1a	6a

Hasil Kompresi

Nilai data yang terdapat pada posisi sebelah kiri matrik Z [0..15].

Table 5.4 Variable X dari proses kompresi percobaan C

Variable X			
DT ARRAY X KE-1	**DT ARRAY X KE-15**	**DT ARRAY X KE-25**	**DT ARRAY X KE**
HSL KOMPRES1=244	HSL KOMPRES1=	HSL KOMPRES1=188	HSL KOMPRES1=
IDX TABEL KE-34	IDX TABEL KE-151	IDX TABEL KE-15	IDX TABEL KE-2
HSL KOMPRES2=103	HSL KOMPRES2=16	HSL KOMPREsi	HSL KOMPRES2=
IDX TABEL KE-34	IDX TABEL KE-151	IDX TABEL KE-15	IDX TABEL KE-2
HSL KOMPRES3 =33	HSL KOMPRES3 =4	HSL KOMPRES3 =43	HSL KOMPRES3
IDX TABEL KE-34	IDX TABEL KE-23	IDX TABEL KE-15	IDX TABEL KE-1
HSL KOMPRES4 =12	HSL KOMPRES4 =13	HSL KOMPRES4 =31	HSL KOMPRES4
HSL KOMPRES5=10	HSL KOMPRES5=2	HSL KOMPRES5=8	HSL KOMPRES5=
IDX TABEL KE-2	IDX TABEL KE-23	IDX TABEL KE-15	IDX TABEL KE-1

Nilai data yang terdapat pada posisi sebelah kanan matrik Z[16..31].

Table 5.5 Variable Y dari proses kompresi percobaan C

Variable Y			
DT ARRAY Y KE-1	**DT ARRAY Y KE-15**	**DT ARRAY Y KE-25**	**DT ARRAY Y KE**
HSL KOMPRES1=40	HSL KOMPRES1=183	HSL KOMPRES1=217	HSL KOMPRES1=
IDX TABEL KE-115	IDX TABEL KE-139	IDX TABEL KE-168	IDX TABEL KE-5
HSL KOMPRES2=98	HSL KOMPRES2=98	HSL KOMPRES2=92	HSL KOMPRES2=
IDX TABEL KE-115	IDX TABEL KE-139	IDX TABEL KE-168	IDX TABEL KE-5
HSL KOMPRES3=38	HSL KOMPRES3=32	HSL KOMPRES3=57	HSL KOMPRES3=
IDX TABEL KE-115	IDX TABEL KE-11	IDX TABEL KE-40	IDX TABEL KE-5
HSL KOMPRES4=30	HSL KOMPRES4=9	HSL KOMPRES4=29	HSL KOMPRES4=
IDX TABEL KE-51	IDX TABEL KE-11	IDX TABEL KE-40	IDX TABEL KE-5
HSL KOMPRES5=9	HSL KOMPRES5=7	HSL KOMPRES5=5	HSL KOMPRES5=
IDX TABEL KE-19	IDX TABEL KE-11	IDX TABEL KE-8	IDX TABEL KE-2

Tabel 5.6 Hasil keluaran SRes (*Signal Response*) dalam biner percobaan C

Hasil SRes				
sresx[0]LSB:1	sresx[1]LSB:1	sresx[2]LSB:0	sresx[3]LSB:0	sresx[4]LSB:0
sresx[0]LSB:1	sresx[1]LSB:1	sresx[2]LSB:0	sresx[3]LSB:1	sresx[4]LSB:1
sresx[0]LSB:1	sresx[1]LSB:0	sresx[2]LSB:0	sresx[3]LSB:0	sresx[4]LSB:0
sresx[0]LSB:1	sresx[1]LSB:0	sresx[2]LSB:1	sresx[3]LSB:0	sresx[4]LSB:0

sresx[5]LSB:0	sresx[6]LSB:0	sresx[7]LSB:1
sresx[5]LSB:1	sresx[6]LSB:0	sresx[7]LSB:0
sresx[5]LSB:1	sresx[6]LSB:0	sresx[7]LSB:0
sresx[5]LSB:0	sresx[6]LSB:0	sresx[7]LSB:0

SRES = FC144608

5.2.2 Karakteristik unjuk kerja proses autentikasi terhadap usaha pemalsuan Ki dan Rand.

Uji coba karakteristik unjuk kerja proses autentikasi terhadap usaha pemalsuan Ki dan Rand dilakukan untuk mengetahui kondisi kegagalan terjadinya autentikasi, Uji coba dilakukan dengan menggunakan Ki dan Rand yang dimanipulasi/dipalsukan dari nilai yang diberikan oleh MSC.

Uji coba D, unjuk kerja proses autentikasi terhadap usaha pemalsuan/manipulasi Ki

D. Unjuk kerja algoritma A3 menggunakan program yang dibuat dengan masukan Ki yang beda dari masukan sebelumnya dan Rand yang sama dengan masukan sebelumnya, untuk mengetahui pengaruh keluaran yang dihasilkan sebagai referensi analisis.

Input Melalui Keypad

Ki =	46	5B	5C	E8	B1	99	B4	9F	AA	5F	0A	2E	E2	38	A6	BC
Rand =	9F	7C	8D	2	1A	BC	F4	DB	21	3C	CF	F0	7C	F7	1A	6A

Hasil Kompresi

Nilai data yang terdapat pada posisi sebelah kiri matrik Z [0..15].

Tabel 5.7 Hasil variable X dari proses kompresi percobaan D

Variable X			
DT ARRAY X KE-1	**DT ARRAY X KE-15**	**DT ARRAY X KE-25**	**DT ARRAY X KE**
HSL KOMPRES1=189	HSL KOMPRES1=132	HSL KOMPRES1=121	HSL KOMPRES1=
IDX TABEL KE-173	IDX TABEL KE-93	IDX TABEL KE-127	IDX TABEL KE-2
HSL KOMPRES2=54	HSL KOMPRES2=22	HSL KOMPRES2=75	HSL KOMPRES2=
IDX TABEL KE-173	IDX TABEL KE-93	IDX TABEL KE-127	IDX TABEL KE-2
HSL KOMPRES3 =42	HSL KOMPRES3 =60	HSL KOMPRES3 =7	HSL KOMPRES3 =
IDX TABEL KE-45	IDX TABEL KE-93	IDX TABEL KE-127	IDX TABEL KE-1
HSL KOMPRES4 =22	HSL KOMPRES4 =3	HSL KOMPRES4 =19	HSL KOMPRES4 =
HSL KOMPRES5=2	HSL KOMPRES5=13	HSL KOMPRES5=12	HSL KOMPRES5=
IDX TABEL KE-13	IDX TABEL KE-29	IDX TABEL KE-31	IDX TABEL KE-8

Nilai data yang terdapat pada posisi sebelah kanan matrik Z[16..31].

Tabel 5.8 Hasil keluaran Variable Y dari proses kompresi percobaan D

Variable Y			
DT ARRAY Y KE-1	**DT ARRAY Y KE-15**	**DT ARRAY Y KE-25**	**DT ARRAY Y KE**
HSL KOMPRES1=204	HSL KOMPRES1=115	HSL KOMPRES1=180	HSL KOMPRES1=
IDX TABEL KE-137	IDX TABEL KE-23	IDX TABEL KE-136	IDX TABEL KE-5
HSL KOMPRES2=30	HSL KOMPRES2=10	HSL KOMPRES2=44	HSL KOMPRES2=
IDX TABEL KE-137	IDX TABEL KE-23	IDX TABEL KE-136	IDX TABEL KE-5
HSL KOMPRES3=51	HSL KOMPRES3=4	HSL KOMPRES3=39	HSL KOMPRES3=
IDX TABEL KE-9	IDX TABEL KE-23	IDX TABEL KE-8	IDX TABEL KE-5
HSL KOMPRES4=19	HSL KOMPRES4=13	HSL KOMPRES4=17	HSL KOMPRES4=
IDX TABEL KE-9	IDX TABEL KE-23	IDX TABEL KE-8	IDX TABEL KE-5
HSL KOMPRES5=0	HSL KOMPRES5=2	HSL KOMPRES5=5	HSL KOMPRES5=
IDX TABEL KE-9	IDX TABEL KE-23	IDX TABEL	IDX TABEL KE-1

Tabel 5.9 Hasil keluaran SRes (*Signal Response*) dalam biner percobaan D

Hasil SRes				
sresx[0]LSB:1	sresx[1]LSB:1	sresx[2]LSB:1	sresx[3]LSB:0	sresx[4]LSB:1
sresx[0]LSB:1	sresx[1]LSB:0	sresx[2]LSB:0	sresx[3]LSB:0	sresx[4]LSB:1
sresx[0]LSB:1	sresx[1]LSB:1	sresx[2]LSB:1	sresx[3]LSB:1	sresx[4]LSB:1
sresx[0]LSB:1	sresx[1]LSB:0	sresx[2]LSB:1	sresx[3]LSB:1	sresx[4]LSB:0

sresx[5]LSB:0	sresx[6]LSB:1	sresx[7]LSB:1
sresx[5]LSB:1	sresx[6]LSB:0	sresx[7]LSB:0
sresx[5]LSB:1	sresx[6]LSB:0	sresx[7]LSB:1
sresx[5]LSB:0	sresx[6]LSB:1	sresx[7]LSB:0

SRES = FAB3E69A

Uji coba E, unjuk kerja proses autentikasi terhadap usaha pemalsuan/manipulasi Rand

E. Unjuk kerja algoritma A3 menggunakan program yang dibuat dengan masukan Ki yang sama dari masukan sebelumnya dan Rand yang beda dengan masukan sebelumnya, untuk mengetahui pengaruh keluaran yang dihasilkan sebagai referensi analisis.

Input Melalui Keypad

Ki =	fe	c8	6b	a6	eb	70	7e	d0	89	5	75	7b	1b	b4	4b	8f
Rand =	23	55	3c	be	96	37	a8	9d	21	8a	e6	4d	ae	47	bf	35

Hasil Kompresi

Nilai data yang terdapat pada posisi sebelah kiri matrik Z [0..15].

Tabel 5.10 Hasil Variable X dari proses kompresi percobaan E

Variable [X]			
DT ARRAY X KE-1	**DT ARRAY X KE-15**	**DT ARRAY X KE-25**	**DT ARRAY X KE**
HSL KOMPRES1=117	HSL KOMPRES1=53	HSL KOMPRES1=188	HSL KOMPRES1=
IDX TABEL	IDX TABEL KE-19	IDX TABEL KE-15	IDX TABEL KE-1
HSL KOMPRES2=69	HSL KOMPRES2=83	HSL KOMPRES2=43	HSL KOMPRES2=
IDX TABEL KE-184	IDX TABEL KE-19	IDX TABEL KE-15	IDX TABEL KE-1
HSL KOMPRES3 =41	HSL KOMPRES3 =34	HSL KOMPRES3 =43	HSL KOMPRES3 =
IDX TABEL KE-56	IDX TABEL KE-19	IDX TABEL KE-15	IDX TABEL KE-4
HSL KOMPRES4 =11	HSL KOMPRES4 =30	HSL KOMPRES4 =31	HSL KOMPRES4 =
HSL KOMPRES5=5	HSL KOMPRES5=9	HSL KOMPRES5=8	HSL KOMPRES5=
IDX TABEL KE-24	IDX TABEL KE-19	IDX TABEL KE-15	IDX TABEL KE-1

Nilai data yang terdapat pada posisi sebelah kanan matrik Z[16..31].

Tabel 5.11 Hasil Variable Y dari proses kompresi percobaan E

DT ARRAY Y KE-1	DT ARRAY Y KE-15	DT ARRAY Y KE-25	DT ARRAY Y KE
HSL KOMPRES1=207	HSL KOMPRES1=35	HSL KOMPRES1=217	HSL KOMPRES1=
IDX TABEL KE-62	IDX TABEL KE-73	IDX TABEL KE-168	IDX TABEL KE-2
HSL KOMPRES2=105	HSL KOMPRES2=56	HSL KOMPRES2=92	HSL KOMPRES2=
IDX TABEL KE-62	IDX TABEL KE-73	IDX TABEL KE-168	IDX TABEL KE-2
HSL KOMPRES3=16	HSL KOMPRES3=18	HSL KOMPRES3=57	HSL KOMPRES3=
IDX TABEL KE-62	IDX TABEL KE-73	IDX TABEL KE-40	IDX TABEL KE-2
HSL KOMPRES4=22	HSL KOMPRES4=19	HSL KOMPRES4=29	HSL KOMPRES4=
IDX TABEL KE-62	IDX TABEL KE-9	IDX TABEL KE-40	IDX TABEL KE-2
HSL KOMPRES5=15	HSL KOMPRES5=0	HSL KOMPRES5=5	HSL KOMPRES5=
IDX TABEL KE-30	IDX TABEL KE-9	IDX TABEL KE-8	IDX TABEL KE-2

Tabel 5.12 Hasil keluaran SRes (*Signal Response*) dalam biner percobaan E

Hasil SRes				
sresx[0]LSB:1	sresx[1]LSB:1	sresx[2]LSB:0	sresx[3]LSB:0	sresx[4]LSB:0
sresx[0]LSB:1	sresx[1]LSB:0	sresx[2]LSB:0	sresx[3]LSB:0	sresx[4]LSB:0
sresx[0]LSB:0	sresx[1]LSB:0	sresx[2]LSB:0	sresx[3]LSB:0	sresx[4]LSB:0
sresx[0]LSB:1	sresx[1]LSB:0	sresx[2]LSB:1	sresx[3]LSB:0	sresx[4]LSB:1

sresx[5]LSB:0	sresx[6]LSB:1	sresx[7]LSB:1
sresx[5]LSB:0	sresx[6]LSB:0	sresx[7]LSB:0
sresx[5]LSB:0	sresx[6]LSB:0	sresx[7]LSB:1
sresx[5]LSB:1	sresx[6]LSB:0	sresx[7]LSB:0

SRES = D810118A

5.3 ANALISIS

Analisis yang dapat diambil mengenai aspek keamanan yang diterapkan pada proses autentikasi serta rancangan algoritma A3 berdasarkan hasil keluaran simulasi/komputasi diatas adalah sebagai berikut:

Pada percobaan A (Unjuk kerja algoritma A3 dengan windows Excel), memperlihatkan hasil pengolahan proses algoritma A3 di jelaskan secara bertahap karena untuk mengetahui secara jelas fungsi penting dari tahapan-tahapan pengolahan algoritma A3 tersebut.

a. Tahap kompresi berfungsi untuk mengecilkan nilai data masukan dari 2^8 bit menjadi 2^4 bit
b. Tahapan kedua, pembentukan matrik untuk permutasi yang dibentuk dari perubahan byte menjadi bit berfungsi untuk mengecilkan jumlah array dari matrik X [0...31] menjadi X [0...7] atau kapasitas byte, dari 32 byte menjadi 8 byte.
c. Tahapan terakhir, permutasi berfungsi untuk makin memperkecil jumlah array yaitu dari matrik X [0..7] menjadi X [0..3] atau kapasitas byte yang akan dibangkitkan sebagai keluaran SRes dari 8 byte menjadi 4 byte

Percobaan A menganalisis peran penting dari setiap tahapan dari pengolahan algoritma A3 terhadap masukan Ki dan Rand sebesar 32 byte dengan nilai data 2^8 agar bisa membangkitkan SRes sebesar 32 bit adalah:

a. Nilai data 2^8 pada masukan diperkecil menjadi 2^4 dengan menggunakan structur kupu-kupu.
b. Jumlah kapasitas masukan 32 byte di kompresi menjadi 8 byte
c. Jumlah kapasitas 8 byte dikompresi lagi terakhir menjadi 4 byte

Pada percobaan B (Unjuk kerja Algoritma A3 menggunakan mikrokontroller pada sisi pelanggan), Memperlihatkan program algoritma A3 berkerja meggunakan mikrokontroller dengan menghasilkan keluaran 32 bit.

Parameter untuk menyatakan keluaran SRes yang benar di program Algoritma A3 adalah jumlah SRes yang dikeluaran sebesar 32 bit sesuai dengan spesifikasi

ETSI. Maka percobaan B unjuk kerja Algoritma A3 menggunakan mikrokontroller bekerja telah sesuai dengan algoritma A3.

Parameter untuk menyatakan keluaran yang benar di program algoritma A3 untuk autentikasi GSM adalah Jumlah SRes yang dikeluarkan sebesar 32 bit dan nilai byte sama dengan jumlah byte yang ada di jaringan.

Di percobaan B hanya berbicara pada sisi pelanggan, tidak berbicara tentang autentikasi berhasil atau tidak karna disini penekanan terhadap pengujian kebenaran kinerja program yang dibuat menggunakan mikrokontroller.

Percobaan B memperlihatkan keberhasilan kerja program A3 di jalankan di mikrokontroller.

Uji coba B

Ki =	46	5b	5c	e8	b1	99	b4	9f	aa	5f	0a	2e	e2	38	a6	bc
Rand =	23	55	3c	be	96	37	a8	9d	21	8a	e6	4d	ae	47	bf	35

SRES = 95D1CAD2

Pada percobaan C (Uji coba menggunakan Ki dan Rand yang berbeda), memperlihatkan pengujian lebih lanjut atas berfungsinya program yang dibuat, output yang dikeluarkan beda nilai byte nya dikarenakan menggunakan masukan yang berbeda dari percobaan B, apabila terjadi ouput yang sama maka program tidak bekerja sesuai dengan sistem algoritma A3

Uji coba C

Ki =	fe	c8	6b	a6	eb	70	7e	d0	89	5	75	7b	1b	b4	4b	8f
Rand =	9f	7c	8d	2	1a	bc	f4	db	21	3c	cf	f0	c7	f7	1a	6a

SRES = FC144608

Pada percobaan D (Uji coba dengan Ki yang berbeda atau Ki telah dimanulasi sehingga berbeda dengan Ki yang berada pada MSC walaupun masukan Rand yang sama karena Rand dikirim dari MSC)

Pada sisi MSC (Mikrokontroller A) dengan menjalankan algoritma yang sama dengan pada sisi pelanggan (Mikrokontroller B) didapat

.Pada sisi MSC (Mikrokontroller A)

Ki =	fe	c8	6b	a6	eb	70	7e	d0	89	5	75	7b	1b	b4	4b	8f
Rand =	9f	7c	8d	2	1a	bc	f4	db	21	3c	cf	f0	c7	f7	1a	6a

SRES = FC144608

Pada sisi pelanggan (Mikrokontroller B)

Ki =	46	5B	5C	E8	B1	99	B4	9F	AA	5F	0A	2E	E2	38	A6	BC
Rand =	9F	7C	8D	2	1A	BC	F4	DB	21	3C	CF	F0	7C	F7	1A	6A

SRES = FAB3E69A

Pada uji coba D, memperlihatkan uji coba yang menyatakan proses autentikasi yang gagal, dikarenakan output pada sisi pelanggan dengan ouput pada sisa jaringan berbeda, Output yang sesuai dengan keluaran yang diharapkan oleh paremeter autentikasi GSM dinyatakan dengan nilai byte SRes yang dihasilkan oleh pelanggan sama pada output nilai byte SRes pada sisi jaringan, menghasilkan output yang sesuai dengan parameter keluaran algoritma A3 yang benar sehingga kondisi ini dinyatakan autentikasi tidak diterima.

Pada simulasi ini dianggap intruder berusaha memalsukan ataupun memanipulasi Ki dari pelanggan yang sedang disadap tersebut.

Jika kedua SRes yang dibandingkan di dalam jaringan sama, maka jaringan akan mengirimkan indikasi yang menandakan bahwa hubungan komunikasi dapat

dilakukan. Tetapi jika kedua SRes berbeda diakibatkan adanya masukan Ki yang dipalsukan/dimanipulasi ternyata tidak sesuai dengan Ki yang di sisi MSC, .maka jaringan menggagalkan hubungan komunikasi yang akan di bangun oleh pelanggan yang tidak berhak tersebut.

Dari uji coba ini program memperlihatkan tingkat keamanan dari suatu sistem autentikasi GSM, dimana Ki yang akan di duplikat harus benar-benar terdapat pada memori SIM card.

Nilai Ki yang tersimpan pada SIM card merupakan kunci pengkloningan, untuk mengatasi ini jaringan GSM memiliki gelombang penjegal untuk jenis serangan ini, mekanismenya yaitu jika dua telephon dengan ID yang sama dijalankan secara bersamaan, dan jaringan GSM mendeteksinya, mendeteksi ada telepon yang'sama' pada lokasi yang berbeda, maka secara otomatis jaringan GSM akan menutup *account* tersebut.

Pada uji coba E memperlihatkan Uji coba dengan Rand yang berbeda, Uji coba ini di kondisi kenyataannya mungkin tidak akan terjadi, pemalsuan pada sisi masukan Rand pada sisi pelanggan akan sulit dilakukan dikarenakan Rand ditentukan oleh MSC.

.Pada sisi MSC (Mikrokontroller A)

Ki =	fe	c8	6b	a6	eb	70	7e	d0	89	5	75	7b	1b	b4	4b	8f
Rand =	9f	7c	8d	2	1a	bc	f4	db	21	3c	cf	f0	c7	f7	1a	6a

SRES = FC144608

Pada sisi pelanggan (Mikrokontroller B)

Ki =	fe	c8	6b	a6	eb	70	7e	d0	89	5	75	7b	1b	b4	4b	8f
Rand =	23	55	3c	be	96	37	a8	9d	21	8a	e6	4d	ae	47	bf	35

SRES = D810118A

Perubahan nilai di salah satu masukan algoritma A3 mengakibatkan nilai SRes keluarannya tidak benar di lihat dari parameter keluaran yang diharapkan untuk autentikasi GSM yaitu tidak hanya jumlah byte yang sama pada sisi pelanggan dengan MSC, tetapi juga nilai byte juga harus sama. Jika keluaran SRes tersebut tidak benar maka akan dilakukan proses pengulangan proses autentikasi dari awal kembali dengan diawali dari pengiriman Rand dari MSC.

Terlihat pada semua hasil uji coba, nilai keluaran simulasi SRes diperoleh dengan pola (nilai) yang acak /tidak tentu. Hal ini dimungkinkan dengan adanya metode pengacakan secara dijital yang diimplementasikan dalam suatu bentuk kompresi terhadap data-data masukan yang terdiri dari Ki dan Rand.

BAB 6
KESIMPULAN

Berdasarkan dari rancang bangun simulasi dan prinsip kerja sistem yang telah di teliti maka dapat disimpulkan, bahwa:

1. Uji coba rancang bangun simulasi memperlihatkan tingkat keamanan dari suatu sistem autentikasi GSM, dimana Ki yang akan di duplikat harus benar-benar terdapat pada memori SIM card.Adapun uji coba yang ada menyimpulkan;
2. Percobaan A, Komputasi algoritma A3 dapat juga diperhitungkan secara manual.
3. Percobaan B dan C, memperlihatkan unjuk kerja dari algoritma A3 dalam mengkompresi data yang ada pada kedua masukkan dari triplet autentikasi dengan cara:
   a. Terjadinya kompresi nilai data 2^8 menjadi 2^4 dengan menggunakan struktur kupu-kupu.
   b. Terjadi kompresi jumlah kapasitas masukan 32 byte menjadi 8 byte
   c. Terjadi kompresi jumlah kapasitas 8 byte menjadi 4 byte (Nilai SRes)
4. Percobaan B dan C, memperlihatkan rancang bangun simulasi telah bekerja berdasarkan algoritma A3 yang menghasilkan keluaran sesuai dengan standart spesifikasi ETSI.
5. Percobaan D, memperlihatkan rancang bangun simulasi yang menghasilkan output keluaran yang berbeda antara pelanggan dengan MSC yang disebabkan masukan Ki dipalsukan/dimanipulasi, mengakibatkan proses autentikasi tidak berhasil dan pelanggan tidak bisa mengakses layanan GSM
6. Percobaan E. Memperlihatkan rancang bangun simulasi yang menghasilkan output keluaran yang berbeda antara pelanggan dengan MSC yang disebabkan masukan Rand dipalsukan/dimanipulasi, mengakibatkan proses autentikasi tidak berhasil dan pelanggan tidak bisa mengakses layanan GSM. di kondisi kenyataannya mungkin sulit terjadi, pemalsuan pada sisi masukan Rand pada sisi pelanggan akan sulit dilakukan dikarenakan Rand ditentukan oleh operator.

DAFTAR ACUAN

[1] Aditya, Randy (2003). **“** Skema dan Arsitekture digital *signature* untuk aplikasi *mobile* ”. Diakses 01 Oktober 2008, dari Institut Teknologi Bandung.
http://www.itb.ac.id

[2] Ratih (2003). **“** Studi dan Perbandingan simcard dan kriptografi kunci simetri dan asimetri pada telepon selular ”. Diakses 01 Oktober 2008, dari Institut Teknologi Bandung.
http://www.itb.ac.id

[3] JM Zacharias (2005). **“** *Arsitekture* GSM”. Diakses 01 Oktober 2008,
http://www.jmzacharias.com/GSM.htm

[4] *Uke Kurniawan Usman, Ir, MT*. **“***Global Sistem for Mobile communication* (GSM)*”*, Diakses 01 Oktober 2008, dari STTTELKOM, Bandung.
http://www.stttelkom.ac.id

[5] *Uke Kurniawan Usman, Ir, MT*. **“** Sarana otentikasi dan keamanan bagi pengguna sistem selular CDMA 2000-1X*”*, Diakses 01 Oktober 2008, dari STTTELKOM, Bandung.
http://www.stttelkom.ac.id

[6] Ariadi . “ Implementasi rancangan algoritma A3/A8 pada model simulasi proses autentikasi sistem telepon bergerak selular digital.”. Skripsi , Program Sarjana Fakultas Teknik UI, Depok, 2007, hal. 19

[7] Atmel Corporation (2000). *AT89S51 Datasheet.* Diakses 07 Oktober 2008’ dari Atmel.
http://www.atmel.com

[8] Setiawan, Rachmad (2006). ***“Mikrokontroler MCS-51”***, Graha Ilmu Edisi Pertama, Yogyakarta

[9] Barry B. Brey (2005). " *Mikroprocessors : 8086/ 8088, 80186/80188, 80286, 80386, 80486, Pentium, Prosesor Pentium Pro, Pentium II, Pentium III, dan Pentium 4 Edisi keenam ",* Ed.I, ANDI, Yogyakarta.

[10] *Beyond Logic* (2005). **"***Schema of* LCD". Diakses 07 Oktober 2008, http://www.beyondlogic.org/parlcd/parlcd.htm.

[11] Dean Fathony Alfatwa (2003). **"** Kartu cerdas (*Smart card*) dan hubungannya dengan kriptografi". Diakses 01 Oktober 2008, dari Institut Teknologi Bandung.
http://www.itb.ac.id

[12] Wang Kleiner. **"** GSM-Cloning.ppt". Diakses 8 Desember 2008.

[13] J.R. Rao, P. Rohatgi, H. Scherzer, S. Tinguely (2002) *Partitioning Attacks: Or How to Rapidly Clone GSM Cards.* Diakses 07 Oktober 2008, http://csdl.computer.org/comp/proceedings/sp/2002/1543/00/15430031abs.htm

DAFTAR PUSTAKA

Didin Wahyudin (2007).**"***Belajar Mudah Mikrokontroler AT89S52 dengan Bahasa BASIC Menggunakan BASCOM-8051"*, Penerbit ANDI, Ed. I, Yogyakarta.

Sudmeyer, Philipp (2006).*" A performance oriented implementation of COMP128"*, RuhrUniversity Bochum, Jerman.

Sin, Susan. "COMP128." http://calliope.uwaterloo.ca/ssjsin/COMP128.pdf tanggal akses 20 November 2008

LAMPIRAN

TABEL AUTENTIKASI

TABEL 512

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	→ Indeks ke
102,	177 ,	186,	162,	2 ,	156 ,	112,	75,	55,	25,	8 ,	12 ,	251,	193,	246,	188,	→ Nilai data kompresi

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
109 ,	213,	151,	53,	42,	79,	191 ,	115,	233,	242,	164,	223,	209 ,	148,	108,	161,

32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
252 ,	37,	244,	47,	64,	211 ,	6,	237,	185,	160,	139 ,	113,	76,	138,	59,	70,

48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
67	, 26,	13,	157,	63,	179,	221 ,	30,	214,	36,	166 ,	69,	152,	124,	207,	116,

64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
247 ,	194,	41,	84,	71,	1 ,	49,	14,	95,	35,	169 ,	21,	96,	78,	215,	225,

80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
182 ,	243,	28,	92,	201,	118 ,	4,	74 ,	248,	128,	17,	11 ,	146,	132,	245,	48,

96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
149 ,	90,	120,	39,	87 ,	230,	106 ,	232,	175 ,	19 ,	126,	190 ,	202 ,	141 ,	137,	176,

112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
250 ,	27 ,	101,	40 ,	219 ,	227,	58 ,	20,	51 ,	178 ,	98,	216 ,	140,	22 ,	32 ,	121,

128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
61 ,	103 ,	203 ,	72 ,	29,	110 ,	85,	212 ,	180 ,	204 ,	150,	183 ,	15,	66 ,	172 ,	196,

144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
56	, 197 ,	158,	0,	100 ,	45 ,	153 ,	7 ,	144 ,	222 ,	163,	167 ,	60,	135 ,	210 ,	231,

160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175

```
174 ,165 , 38,249 ,224, 34 ,220 ,229,217 ,208 ,241, 68 ,206,189 ,125 ,255,

 176  177  178  179  180  181  182  183  184  185  186  187  188  189  190  191
239 , 54 ,168, 89,123 ,122 , 73 ,145 ,117,234,143 , 99 ,129,200 ,192, 82 ,

 192  193  194  195  196  197  198  199  200  201  202  203  204  205  206  207
104 ,170 ,136,235 , 93, 81 ,205 ,173,236 , 94 ,105, 52 , 46,228 ,198 , 5 ,

 208  209  210  211  212  213  214  215  216  217  218  219  220  221  222  223
57  ,254 , 97,155 ,142,133 ,199 ,171 ,187, 50 , 65,181 ,127,107 ,147 ,226,

 224  225  226  227  228  229  230  231  232  233  234  235  236  237  238  239
184 ,218 ,131 , 33, 77, 86 , 31 , 44, 88 , 62 ,238, 18 , 24, 43 ,154 , 23,

 240  241  242  243  244  245  246  247  248  249  250  251  252  253  254  255
80  ,159 ,134 ,111, 9 ,114 , 3 , 91  ,16 ,130, 83 , 10,195 ,240 ,253 ,119,

 256  257  258  259  260  261  262  263  264  265  266  267  268  269  270  271
177 ,102 ,162,186 ,156,  2 , 75 ,112, 25 , 55, 12 , 8 ,193 ,251 ,188 ,246,

 272  273  274  275  276  277  278  279  280  281  282  283  284  285  286  287
213 ,109 , 53 ,151, 79, 42 ,115 ,191 ,242,233 ,223 ,164,148,209 ,161 ,108,

 288  289  290  291  292  293  294  295  296  297  298  299  300  301  302  303
37 , 252 , 47,244 ,211, 64, 237,  6 ,160 ,185 ,113,139, 138, 76, 70,  59,

 304  305  306  307  308  309  310  311  312  313  314  315  316  317  318  319
26 ,  67 ,157, 13 ,179, 63 , 30 ,221, 36 ,214, 69 ,166 ,124,152 ,116 ,207,

 320  321  322  323  324  325  326  327  328  329  330  331  332  333  334  335
194 ,247 , 84, 41 , 1 , 71 , 14 , 49, 35, 95, 21  ,169, 78, 96  ,225 ,215,

 336  337  338  339  340  341  342  343  344  345  346  347  348  349  350  351
243 ,182 , 92, 28 ,118,201 , 74 , 4 ,128 ,248, 11 , 17 ,132 ,146 ,48 ,245,

 352  353  354  355  356  357  358  359  360  361  362  363  364  365  366  367
```

```
90  ,149 , 39,120 ,230, 87 ,232, 106, 19 ,175 ,190 ,126 ,141,202,176,137,

 368  369  370  371  372  373  374  375  376  377  378  379  380  381  382  383
27  ,250 , 40,101 ,227,219 , 20, 58 ,178 , 51,216 , 98 , 22 ,140,121, 32,

 384  385  386  387  388  389  390  391  392  393  394  395  396  397  398  399
103 , 61 , 72,203 ,110, 29 ,212 , 85,204 ,180 ,183,150 , 66, 15 ,196 ,172,

 400  401  402  403  404  405  406  407  408  409  410  411  412  413  414  415
197 , 56 , 0 ,158 , 45,100 , 7 ,153 ,222 ,144 ,167,163 ,135 , 60,231 ,210,

 416  417  418  419  420  421  422  423  424  425  426  427  428  429  430  431
165 ,174 ,249 , 38, 34 ,224,229 ,220 ,208,217 , 68 ,241,189,206 ,255 ,125,

 432  433  434  435  436  437  438  439  440  441  442  443  444  445  446  447
54  ,239 , 89,168 ,122,123 ,145 , 73,234 ,117 , 99,143 ,200,129 , 82, 192,

 448  449  450  451  452  453  454  455  456  457  458  459  460  461  462  463
170 ,104 ,235 ,136, 81, 93 ,173 ,205 , 94,236, 52 ,105,228 , 46 , 5 , 198,

 464  465  466  467  468  469  470  471  472  473  474  475  476  477  478  479
254 , 57 ,155 ,97 ,133,142 ,171 ,199, 50 ,187 ,181 ,65, 107,127 ,226 ,147,

 480  481  482  483  484  485  486  487  488  489  490  491  492  493  494  495
218 ,184,  33,131 , 86 , 77, 44 , 31, 62 , 88 , 18,238 , 43 ,24, 23 , 154,

 496  497  498  499  500  501  502  503  504  505  506  507  508  509  510  511
159  ,80 ,111,134 ,114, 9  , 91 , 3 ,130,  16 ,10 , 83 ,240 ,195,119 ,253
```

TABEL 256

```
 0   1   2   3   4   5   6   7   8   9   10  11  12  13  14  15
19, 11, 80, 114, 43, 1 , 69, 94, 39, 18, 127,1 17, 97,  3, 85, 43,

 16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31
27, 124, 70, 83, 47, 71, 63, 10,  47, 89, 79,  4, 14, 59, 11,  5,

 32  33  34  35  36  37  38  39  40  41  42  43  44  45  46  47
35, 107,103, 68, 21, 86, 36, 91, 85, 126, 32, 50,109, 94, 120,  6,

 48  49  50  51  52  53  54  55  56  57  58  59  60  61  62  63
53, 79, 28,  45, 99, 95, 41,  34, 88, 68, 93, 55, 110,125,105, 20,

 64  65  66  67  68  69  70  71  72  73  74  75  76  77  78  79
90, 80, 76, 96,  23, 60, 89, 64, 121, 56, 14, 74, 101, 8 , 19, 78,

 80  81  82  83  84  85  86  87  88  89  90  91  92  93  94  95
76, 66 ,104, 46,111, 50, 32,  3,  39,  0, 58, 25, 92,  22, 18, 51,

 96  97  98  99  100 101 102 103 104 105 106 107 108 109 110 111
57, 65, 119,116, 22, 109, 7 ,  86, 59,  93,  62,110,  78, 99,  77, 67,

112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127
12, 113, 87,   98,102,  5,  88, 33,  38, 56,  23,  8,   75, 45,  13, 75,

128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143
95,  63, 28,  49, 123, 120, 20, 112, 44, 30,  15,  98, 106, 2,  103, 29,

144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159
82, 107, 42, 124, 24,  30,  41, 16, 108, 100, 117, 40, 73,  40,  7,  114,

160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175
82, 115,  36, 112, 12,102, 100, 84,  92,  48, 72,  97,  9,  54, 55,  74,
```

```
 176  177  178  179  180  181  182  183  184  185  186  187  188  189  190  191
 113,123, 17,  26, 53,  58,  4,   9,  69, 122, 21, 118, 42,  60,  27, 73,

 192  193  194  195  196  197  198  199  200  201  202  203  204  205  206  207
 118,125,  34, 15,  65, 115, 84,  64, 62, 81,  70,  1,   24,111, 121, 83,

 208  209  210  211  212  213  214  215  216  217  218  219  220  221  222  223
 104, 81, 49, 127, 48, 105,  31, 10,  6,  91,  87, 37,  16,  54, 116, 126,

 224  225  226  227  228  229  230  231  232  233  234  235  236  237  238  239
 31, 38,  13,  0,  72,  106, 77, 61, 26,  67,  46, 29,  96, 37,  61,  52,

 240  241  242  243  244  245  246  247  248  249  250  251  252  253  254  255
101, 17,  44,  108, 71, 52,  66, 57,  33,  51, 25,  90,  2,  119,122, 35
```

TABEL 128

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
52,	50,	44,	6,	21,	49,	41,	59,	39,	51,	25,	32,	51,	47,	52,	43,

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
37,	4,	40,	34,	61,	12,	28,	4,	58,	23,	8,	15,	12,	22,	9,	18,

32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
55,	10,	33,	35,	50,	1,	43,	3,	57,	13,	62,	14,	7,	42,	44,	59,

48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
62,	57,	27,	6,	8,	31,	26,	54,	41,	22,	45,	20,	39,	3,	16,	56,

64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
48,	2,	21,	28,	36,	42,	60,	33,	34,	18,	0,	11,	24,	10,	17,	61,

80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
29,	14,	45,	26,	55,	46,	11,	17,	54,	46,	9,	24,	30,	60,	32,	0,

96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
20,	38,	2,	30,	58,	35,	1,	16,	56,	40,	23,	48,	13,	19,	19,	27,

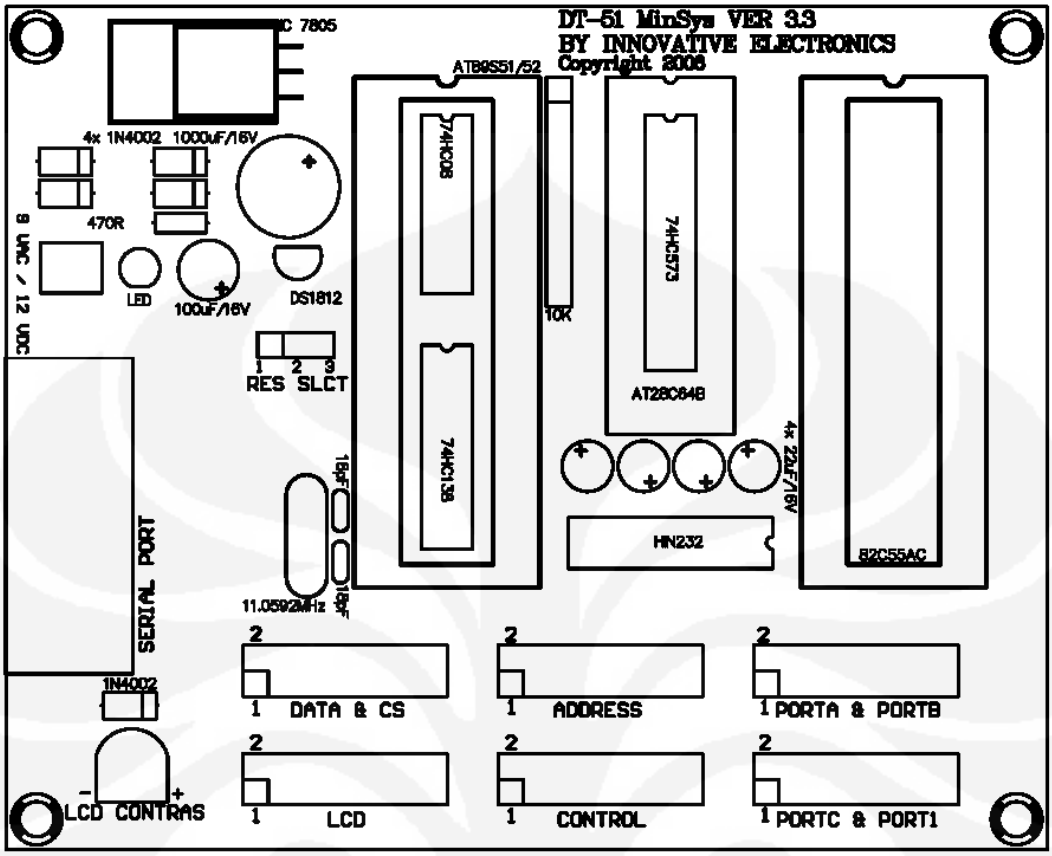
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
31,	53,	47,	38,	63,	15,	49,	5,	37,	53,	25,	36,	63,	29,	5,	7

TABEL 64

```
 0   1   2   3   4   5   6   7   8   9   10  11  12  13  14  15
1,  5,  29,  6,  25, 1,  18, 23, 17,  19, 0,  9,  24, 25,  6,  31,

 16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31
28, 20,  24, 30, 4,  27,  3, 13,  15, 16, 14, 18,  4,  3,  8,  9,

 32  33  34  35  36  37  38  39  40  41  42  43  44  45  46  47
20,  0, 12,  26, 21,  8, 28,  2, 29,  2, 15,  7,  11,  22, 14, 10,

 48  49  50  51  52  53  54  55  56  57  58  59  60  61  62  63
17, 21, 12,  30, 26, 27, 16, 31,  11, 7,  13, 23, 10,  5,  22, 19
```

TABEL 32

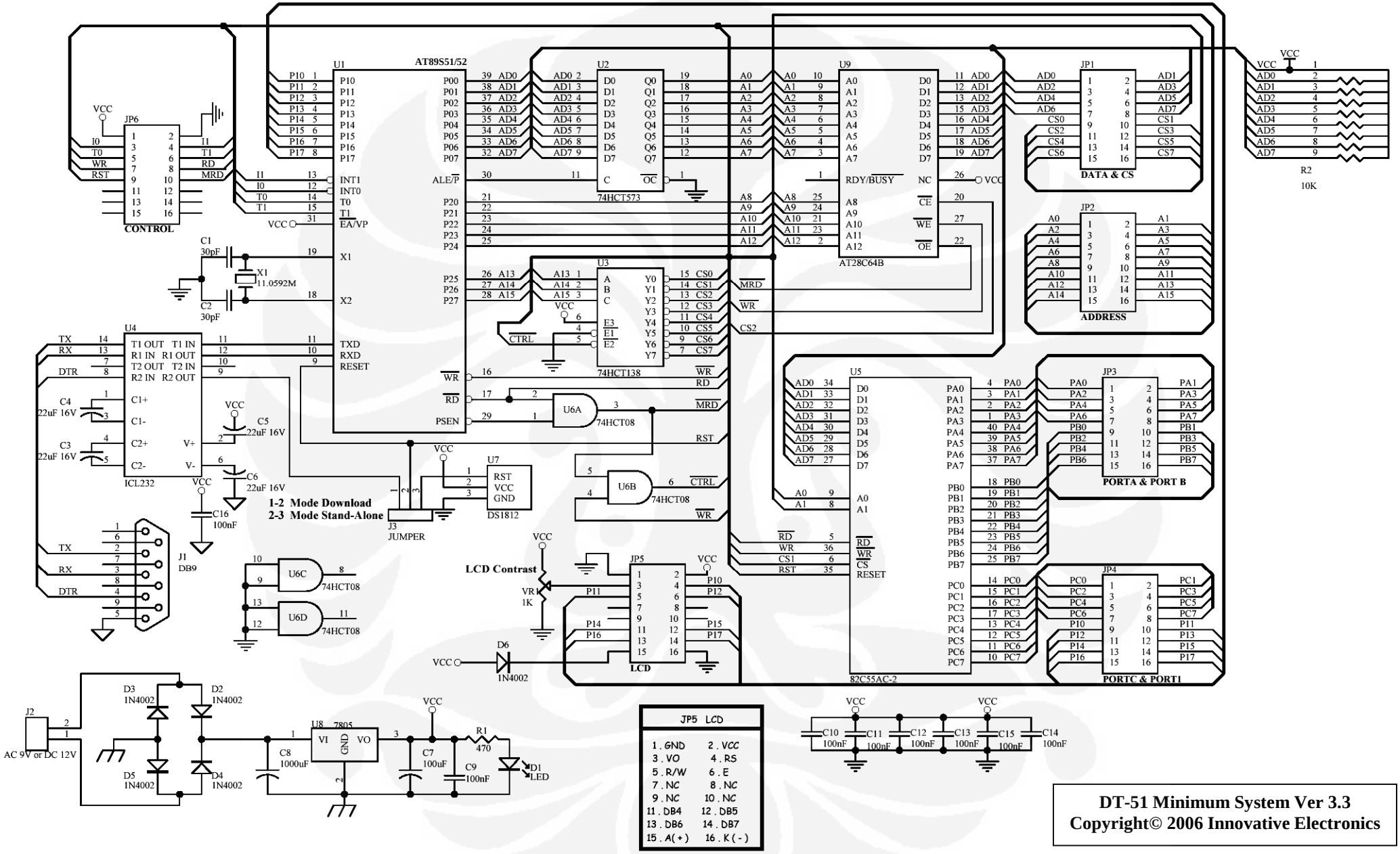
```
  0   1   2   3   4   5   6   7   8   9   10  11  12  13  14  15
 15, 12, 10,  4,  1 , 14, 11,  7,  5,  0,  14,  7,  1,  2, 13,  8,

  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31
10 ,  3 , 4 , 9 , 6 , 0  , 3 , 2 , 5 , 6  , 8, 9 ,  11, 13, 15, 12
```



Gambar 1-1
Tata Letak DT-51 Minimum System ver 3.3

Koneksi Kabel Serial DT-51 Minimum System ver 3.3

PC Serial Port Connector		DT-51 Minimum System ver 3.3 Serial Port Connector
DB9 Female	DB25 Female	DB9 Male
3	2	3
2	3	2
5	7	5
4	20	4



DT-51 Minimum System Ver 3.3
Copyright© 2006 Innovative Electronics