SISTEM PENGAMANAN DATA SIDIK JARI MENGGUNAKAN ALGORITMA AES PADA SISTEM KEPENDUDUKAN BERBASIS *RADIO FREQUENCY IDENTIFICATION* (RFID)

I Gede Andika Putra[1],I Made Widhi Wirawan[2]

Program Studi Teknik Informatika, Jurusan Ilmu Komputer
Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Udayana
Email :igede.andika@cs.unud.ac.id[1], made_widhi@cs.unud.ac.id[2]

ABSTRACT

Kebutuhan manusia akan perangkat informasi dan komunikasi seakan menjadi kebutuhan yang tidak terpisahkan dalam kehidupan sehari-hari. teknologi RFID adalah proses identifikasi seseorang atau objek dengan menggunakan frekuensi transmisi radio. Keamanan data sidik jari penduduk pada *tag RFID* ini merupakan hal yang sangat penting untuk dilakukan. Metode kriptografi menjadi salah satu pilihan dalam pengamanan untuk menghindari jika terjadinya ancaman penyalahgunaan kartu identitas penduduk oleh orang yang tidak berhak.

Objek suatu pengamanan dalam hal ini adalah data sidik jari penduduk yang akan disimpan dalam memori yang terkandung dalam *tag RFID Mifare 1K*. Data yang akan dituliskan ke dalam memory tag di rubah ke bentuk yang sulit dimengerti menurut proses *enkripsi* algoritma AES. Sedangkan dalam proses pembacaan tag akan dijalan kan proses *dekripsi* untuk mengetahui data identitas penduduk yang tersekripsi menjadi data asli.

Metode Algoritma AES dapat memberikan keamanan pada sistem kependudukan berbasis RFID. Bedasarkan pengujian RMS yang telah dilakukan data sidik jari yang diamankan dalam tag RFID tidak dapat digunakan oleh penduduk yang tidak berhak. Disamping itu pada sistem ini dilakukan proses dekripsi untuk menampilkan data penduduk.

Kata kunci : *RFID (Radio Frequecy Identification), Algoritma AES, Sidik Jari, Keamanan RFID.*

1. PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Perkembangan teknologi informasi dan komunikasi dari waktu ke waktu kian meningkat. Kebutuhan manusia akan perangkat informasi dan komunikasi seakan menjadi kebutuhan yang tidak terpisahkan dalam kehidupan sehari-hari. Inovasi yang terjadi dalam bidang ini senantiasa berkembang secara dinamis. Salah satu contohnya adalah teknologi RFID.

RFID adalah proses identifikasi seseorang atau objek dengan menggunakan frekuensi transmisi radio. RFID menggunakan frekuensi radio untuk membaca informasi dari sebuah perangkat kecil yang disebut tag atau transponder (Transmitter + Responder). *Tag* RFID akan mengenali diri sendiri ketika mendeteksi sinyal dari perangkat yang kompatibel, yaitu pembaca RFID (RFID *Reader)*

Salah satu pemanfaatan RFID adalah pada Kartu Identitas Penduduk. Untuk menghindari terjadinya kloning data digital dan penyalah gunaan terhadap kartu identitas penduduk perlu diamankannya suatu data dengan kriptografi.

Kriptografi merupakan salah satu solusi untuk menjamin keamanan dari suatu data yaitu dengan menyandikan isi informasi menjadi isi yang sulit bahkan tidak dipahami dengan cara melalui proses enkripsi *(encryption)*, dan untuk memperoleh kembali informasi yang asli dilakukan proses dekripsi *(decryption)*, disertai dengan menggunakan kunci yang benar. Tujuan dari sistem kriptografi yang terkait dengan aspek keamanan suatu sistem informasi, kerahasian(*privacy*), integritas (*Integrity*), otentikasi (*Authentication*), dan pembuktian yang tidak bias mengelak (*Non-Repudiation*).(Ariyus Dony, 2008).

Melihat hal ini, peneliti mencoba untuk merancang sistem pengamanan data sidik jari menggunakan algoritma *AES* pada sistem kependudukan berbasis RFID. Algoritma AES merupakan algoritma yang sudah terstandarisasi dan dapat dikatakan

relative murah, cepat dan dapat diterapkan pada sistem RFID(Batbold T, 2006). kedalam bentuk sistem yang dirancang untuk melakukan enkripsi dan dekripsi data sidik jari sehingga bisa melakukan pengamanan terhadap data sidik jari agar dikemudian hari tidak terjadi suatu penyalahgunaan baik data digital kependudukan.

1.2 PERUMUSAN MASALAH

Berdasarkan latar belakang di atas, maka permasalahan yang akan dikaji dalam penelitian ini adalah bagaimana merancang sistem pengamanan data sidik jari menggunakan algoritma *AES* pada sistem kependudukan berbasis RFID.

1.3 BATASAN MASALAH

1. Dalam penelitian ini, lebih difokuskan pada pengamanan data sidik jari pada sistem RFID dengan kasus sistem kependudukan.
2. Alat pemindai yang digunakan adalah *fingerprint u are u* 4500 dan *Reader* RFID digunakan Omnikey 5321CL
3. Akuisisi data citra sidik jari langsung dilakukan oleh alat pemindai, sistem hanya melakukan pengolahan hasil ekstraksi ciri dari data citra yang diperoleh.
4. Pada sistem ini algoritma AES inputan data sidik jari dibatasi masing-masing dibatasi sebanyak 16 byte atau 128 bit. Dan panjang kunci selalu mengikuti ukuran panjang dari *plainteks*.

1.4 TUJUAN PENELITIAN

Adapun tujuan yang hendak dicapai dalam penelitian ini adalah untuk merancang dan mengimplementasikan Algoritma AES untuk pengamanan data sidik jari pada sistem kependudukan berbasis RFID. Penggunaan algoritma AES dalam penelitian ini untuk mengamankan data sidik jari penduduk sebelum disimpan dalam tag RFID.

2. TINJAUAN PUSTAKA

2.1 KRIPTOGRAFI

Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata kriptografi dibagi menjadi dua,yaitu *crypto* dan *graphia*. Crypto berarti *secret* (Rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan/ data dikirim dari suatu tempat ke tempat yang lain

Kriptografi menjadi dasar bagi keamanaan jaringan komputer. Karena yang menjadi pokok dari fungsi komputer dan jaringan adalah data dan informasi. Salah satu cara yang paling banyak digunakan dalam mengamankan data adalah dengan mengguanakan kriptografi. Data-data tersebut diamankan oleh pengirim sehingga orang lain tidak dapat mengenali data tersebut.

2.2 ALGORITMA KRIPTOGRAFI

Algoritma-algoritma kriptogrfi dapat dibedakan menjadi dua macam yaitu simetrik dan asimetrik. Algoritma simetrik (model enkripsi konvensional) merupakan algoritma yang menggunakan satu kunci untuk proses enkripsi dan deskripsi data. Sedangkan algoritma asimetrik (model enkripsi kunci publik) menggunakan kunci yang berbeda dalam proses enkripsi dan deskripsi pesan.

2.3 ALGORITMA *AES*

Dalam kriptografi, Anvanced Encryption Standard (AES), juga dikenal sebagai Rijndael, AES adalah sebuah block cipher yang dijadikan standar enkripsi oleh pemerintah Amerika Serikat. Enkripsi ini diharapkan juga digunakan secara luas di seluruh dunia dan dianalisa secara luas, seperti pada pendahulunya , Data Encryption Standard (DES). Rijndael (AES) diumumkan oleh National Institute of Standards and Technology (NIST) pada tanggal 26 Nopember 2001, setelah lima tahun proses standardisasi. Metode enkripsi ini menjadi standar secara efektif mulai tahun 2002. Pada tahun 2006, AES adalah salah satu algoritma populer yang digunakan dalam kriptografi kunci simetris.

Algoritma AES menggunakan substitusi, permutasi, dan sejumlah putaran yang dikenakan pada tiap blok yang akan dienkripsi / dekripsi. Untuk setiap putarannya, Rijndael menggunakan kunci yang berbeda. Rijndael beroperasi dalam orientasi byte sehingga memungkinkan untuk implementasi algoritma yang efisien ke dalam software dan hardware.

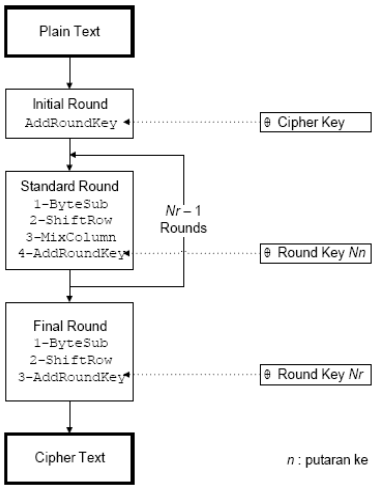
Algoritma *Rijndael* mempunyai 3 parameter sebagai berikut:

1. plainteks: *array* yang berukuran 16 *byte*, yang berisi data masukan.
2. cipherteks: *array* yang berukuran 16 *byte*, yang berisi hasil enkripsi.
3. key: *array* yang berukuran 16 *byte* (untuk panjang kunci 128 bit), yang berisi kunci ciphering (disebut juga *cipher key*).

2.3.1 Proses Enkripsi Algoritma *AES*

Proses yang dilakukan setiap rondenya identik (dari ronde ke-0 sampai dengan ronde ke Nr-1), kecuali untuk ronde terakhir Nr. Proses yang identik tersebut terdiri atas *SubBytes(), ShiftRows(), MixColumns(),* dan *AddRoundKey()*. Sedangkan pada ronde terakhir Nr tidak dilakukan fungsi *MixColumns().*

Array 4 x 4 *byte plaintext* yang disebut *state* dioperasikan XOR dengan kunci, kemudian diolah sebanyak 9 ronde dengan operasi *SubBytes*, *ShiftRows*, *MixColumns*, *AddRoundKey*. Tiap ronde akan memilki round key yang diturunkan dari kunci utama. Pada ronde terakhir (ronde 10) tidak dilakukan proses *MixColumns*, keseluruhan proses enkripsi ini akan mengasilkan *cipher* 4 x 4 *byte*



Gambar.2.1 Skema Enkripsi algoritma *AES*

1. AddRoundKey

Dalam tahap *AddRoundKey*, setiap byte dari *state* digabungkan dengan sebuah byte dari sub-kunci ronde, penggabungan ini menggunakan operasi XOR Untuk setiap rondenya, sebuah sub-kunci diturunkan dari kunci utama menggunakan penjadwalan kunci (*Key Scheduling)*

2. SubBytes

Dalam tahap SubBytes, setiap byte dalam state diganti dengan masukannya dalam sebuah table s-box atau subtitusi box. Operasi ini akan memberikan prinsip non-linieritas pada *cipher*.

3. ShiftRow

Tahap ShiftRows akan menggeser ke kiri secara berputar setiap bytes dalam setiap baris dari *state.* Jumlah pergeseran tiap byte berbeda untuk setiap barisnya. Baris pertama akan tetap pada keadaan semula. Setiap byte dari baris kedua digeser satu langkah ke kiri. Baris ketiga dan keempat digeser ke kiri sebanyak dua dan tiga langkah.

4. MixColumns

Proses *MixColumns* akan beroperasi pada tiap kolom dari tabel *state.* Operasi ini menggabungkan 4 *bytes* dari setiap kolom tabel *state* dan menggunakan transformasi linier.Operasi *Mix Columns* memperlakukan setiap kolom sebagai polinomial 4 suku dalam *Galois field* dan kemudian dikalikan dengan c(x) modulo (x4+1), dimanac(x)=3x3+x2+x+2.

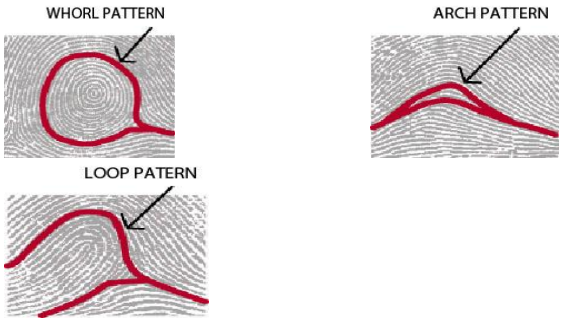
5. Ekspansi Kunci

Algoritma aes melaksanakan kunci-kode dan membuat suatu kunci ekspansi untuk menghasilkan suatu kunci skedul. Kunci ekspansi yang diperlukan AES Nb(Nr+1) kata sehingga bisa digunakan AES 128 bit

2.4 SIDIK JARI

Sidik jari adalah gurat-gurat yang terdapat di kulit ujung jari. Gurat-gurat ini tidak ada yang sama antara satu manusia dengan manusia yang lainnya. walaupun mereka kembar identik. Sehingga sidik jari dapat digunakan untuk mengidentifikasi seseorang misalnya untuk mengidentifikasi pelaku kejahatan ataupun untuk identifikasi pekerja pabrik. (Kaselie, 2009)

Gambar berikut menggambarkan 3 buah tipe pola utama sidik jari.



Gambar 2.2 Beberapa Pola Sidik Jari

titk minusi merupakan titik-titik informasi yang dapat mencirikan suatu sidik jari. beberapa bagian pada sidik jari yang dapat dijadikan sebagai titik minusi antara lain : akhir bukit (*tidge termination*), percabangan (*bifurcation*) ,pulau (*island*) , danau (*lake*), taji (*spur*), persilangan (*crossover*).

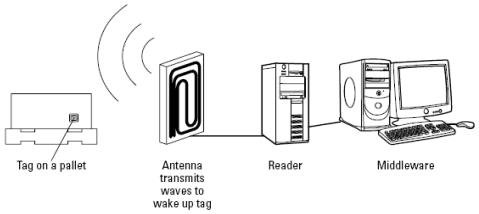
2.5 RFID (RADIO FREQUENCY IDENTIFICATION)

RFID *(Radio Frequency Identification)* adalah sistem teknologi identifikasi berbasis gelombang radio yang dalam proses identifikasinya tidak diperlukan kontak langsung antara *device* pembaca *(Reader)* dengan obyek yang diidentifikasi *(transponder)* yang sering disebut *tag*, dimana *tag* ini adalah *device* pembawa data.

RFID memiliki kelebihan dari pada teknologi pengidentifikasi sebelumnya, seperti barcode. Diantaranya mampu membaca suatu objek data dengan ukuran tertentu tanpa melalui kontak langsung (contacless) dan tidak harus sejajar dengan objek yang dibaca, selain dapat menyimpan informasi pada bagian *tag* RFID sesuai dengan kapasitas penyimpanann.

Sistem RFID terdiri dari empat komponen, di antaranya sebagai berikut : (Erwin, 2004).

1. *Tag* : Ini adalah *device* yang menyimpan informasi untuk identifikasi objek. *Tag* RFID sering juga disebut sebagai *transponder*.
2. Antena : untuk mentransmisikan sinyal frekuensi radio antara pembaca RFID dengan *tag* RFID.
3. *Reade*r RFID: adalah *device* yang kompatibel dengan *tag* RFID yang akan berkomunikasi secara *wireless* dengan *tag*.
4. *Software* Aplikasi: adalah aplikasi pada sebuah *workstation* atau PC *(Personal Computer)* yang dapat membaca data dari *tag* melalui pembaca RFID. Baik *tag* dan pembaca RFID diperlengkapi dengan antena sehingga dapat menerima dan memancarkan gelombang elektromagnetik.



Gambar: 2.3 Sistem RFID

2.5.1 *Tag* RFID

Tag RFID adalah *device* yang dibuat dari rangkaian elektronika dan antena yang terintegrasi di dalam rangkaian tersebut. Rangkaian elektronik dari *tag RFID* umumnya memiliki memori sehingga *tag* ini mempunyai kemampuan untuk menyimpan data. Berdasarkan catu daya *tag*, *tag* RFID dapat digolongkan menjadi tag aktif,tag semi aktif dan tag pasif.

2.5.2 *Reader* RFID

Reader RFID mengirim gelombang radio ke *tag RFID* untuk menanyakan tentang isi data. *Tag RFID* kemudian merespon dengan mengirimkan kembali data yang diminta. *RFID Reader* terhubung melalui *RFID middleware* dengan *database* untuk melakukan pengolahan data. Berikut adalah gambar alat yang dimaksud :

Gambar: 2.4 *Reader* RFID Omnikey 5321CL

3. METODOLOGI PENELITIAN

3.1 OBJEK PENELITIAN

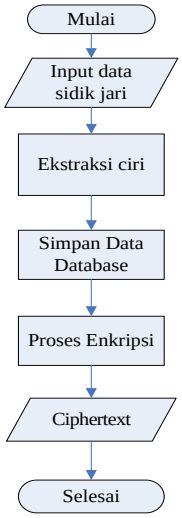
Yang menjadi sebuah objek penelitian adalah data sidik jari penduduk akan disandikan sehingga data tersebut menjadi tidak dapat di pahami. Penyandian data tersebut akan dilakukan dengan menggunakan Algoritma Kriptografi *AES* pada sistem kependudukan berbasis RFID.

3.2 FLOWCHART SISTEM

Beikut ini penjelasan mengenai flowchart yang dibagun, diantaranya :*Flowchart* Enkripsi pada data sidik jari

1. Flowchart proses enkripsi sidik jari

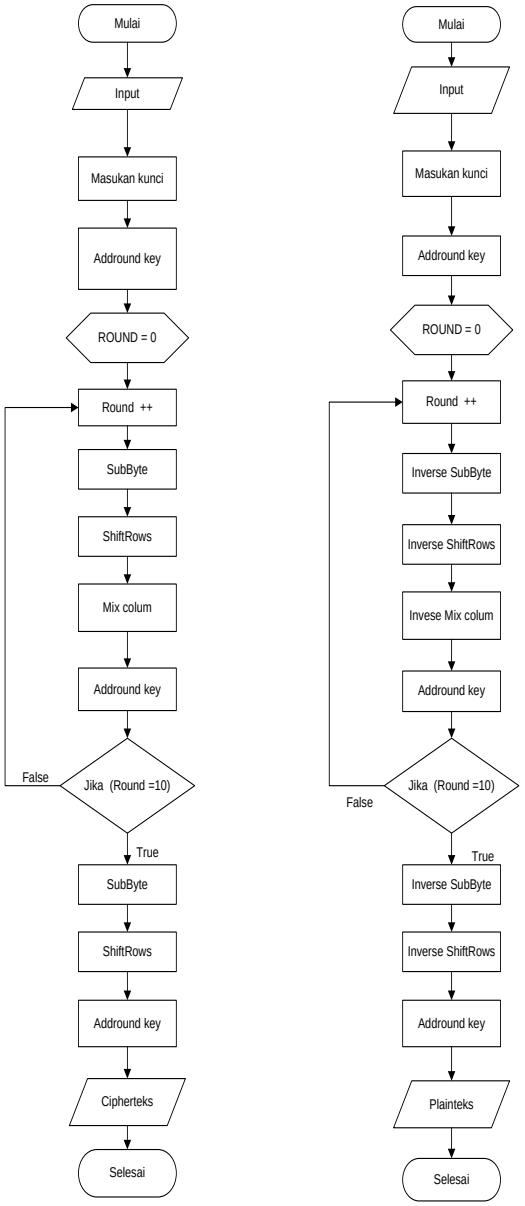
Proses pembelajaran ada beberapa tahapan yang akan dilalui yaitu: Sensor *fingerprint* akan melakukan pembacaan sidik jari yang diinputkan, kemudian sistem akan melakukan ekstraksi sidik jari untuk mendapatkan ciri sidik jari, kemudian hasil ekstraksi ciri sidik jari disimpan ke database. Sebelum data tersebut ditulis ke dalam tag RFID, data sidik jari tersebut dilakukan proses enkripsi.



Gambar 3.5 *Flowchart* proses enkripsi pada data sidik jari

2. Flowchart Enkripsi dan Dekripsi Algoritma AES

Pada gambar 3.6 flowcahrt enkripsi dan dekripsi algoritma AES memiliki dasar pengoprasian pada blok 128 bit dengan pembangkitan kunci 128 bit adalah yang pertama dilakukan adalah SubByte melakuakan substitusi byte dengan menggunakan tabel Substitusi (S-box). ShiftRows melakukan pergesaran baris-baris array secara wrapping. MixColumns mengacak data masing-masing kolom array state. Dan ADdRoundKey melakukan XOR antara state sekarang Roun key. Pada final round proses yang dilakukan adalah SubBytes, ShiftRows, dan AddRoundKey.



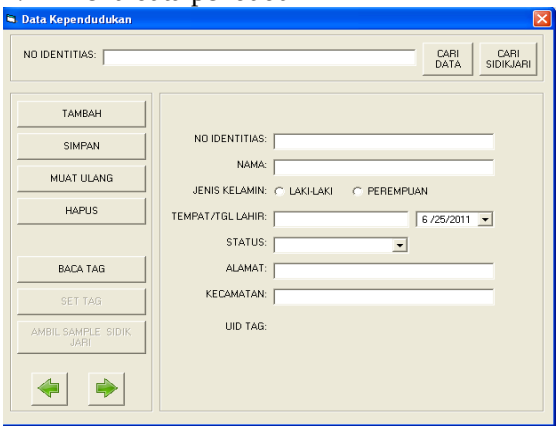
Gambar 3.6 Flowchart enkripsi dan dekripsi Algoritma AES

4. HASIL DAN PEMBAHASAN

4.1 TAMPILAN MENU SISTEM

Ada beberapa menu yang terdapat dalam sistem kependudukan ini. Dalam pembahasan menu sistem `pengguna ini yang dibahas yaitu : menu data penduduk, menu laporan, menu data admin. Berikut ini tampilan yang dijelaskan pada sistem kependudukan :

1. Menu data penduduk



Gambar *:* 4.1 tampilan *inputan data penduduk*

Pada gambar diatas menu pengimputan data pendiuduk dan pengambilan sample sidik jari penduduk.. data sisik jari tersebut akan disimpan dalam database sedangkan yang akan ditulis dalam tag adalah data sidik jari yang sudah dilakukan proses enkripsi(*chiperteks*). Kunci yang digunakan pada proses enkripsi diinputkan oleh penduduk. Dan proses dekripsi kartu tag didekatkan dalam *reader* RFID maka akan keluar menu inputkan kata sandi. Apabila kata sandi benar akan muncul data penduduk.

4.2 PENGUJIAN

4.2.1 Pengujian Algoritma Menggunakan Root Mean Square (RMS)

Untuk mengetahui besarnya perbandingan data saat sebelum dan setelah dienkripsi maka dilakukan uji coba dengan RMS. Adapun rumus yang digunakan adalah :

$$RMS = \frac{1}{n}\sqrt{\sum_{i-1}^{n}(z_i^{'} - z_i)^2}$$

Keterangan :

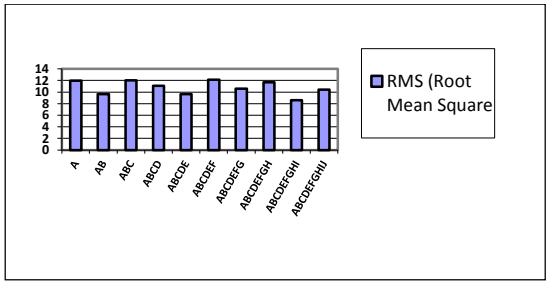
n = jumlah inputan karakter pesan

z_i = nilai *File* sebelum disisipkan dengan pesan teks

$z_i^{'}$ = nilai *File* setelah disisipkan dengan pesan teks

4.2.2.1 Pengujian RMS Berdasarkan Nilai Kunci Yang Berbeda Dengan Data Sidik Jari Yang Sama

Pengujian dilakukan dengan mencari nilai RMS dengan nilai kunci yang berbeda dan data sidik jari yang sama, dalam pengujian ini menggunakan data yang digunakan data sidik jari dan banyaknya kunci yang digunakan sebanyak 10 kunci dan didapat kan grafik sebagai berikut:

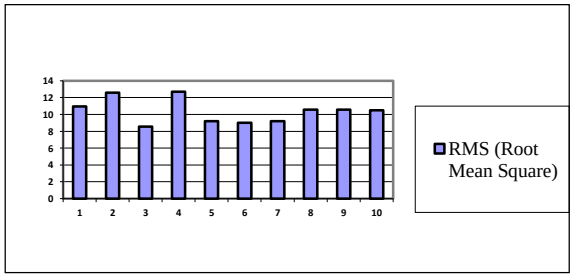


Gambar 4.2 Grafik panjang kunci berbeda dengan data sidik jari sama

Pada pengujian ini Penambahan nilai kunci tidak terlalu berpengaruh terhadap nilai RMS yang dihasilkan dari proses *enkripsi* menggunakan algoritma AES

4.2.2.2 Pengujian RMS Berdasarkan Data Sidik Jari Berbeda Dengan Nilai Kunci Sama

Pengujian dilakukan dengan mencari nilai RMS dengan data sidik jari yang berbeda dan nilai kunci yang sama, dalam pengujian ini data sidik jari yang digunakan diambil dari sample sidik jari penduduk dan nilai kunci yang digunakan adalah AA penggujian dilakukan sebanyak 10 kali pengujian bedasar kan data penduduk. Hasil dari pengujian tersebut di gambarkan dalam bentuk grafik berikut:



Gambar 4.3 Grafik panjang kunci sama dengan data sidik jari berbeda

Perbedaan data sidik jari dengan kunci yang sama tidak berpengaruh nilai RMS yang dihasilkan dari proses menggunakan algoritma AES. Hal ini disebabkan karena algoritma AES setiap putaran menghasilkan kunci yang berbeda

5. KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian yang telah dilakukan adalah sebagai berikut:

1. Bedasarkan penelitian yang dilakukan pada sistem kependudukan berbasis RFID. sistem ini dapat pengamanan data sidik jari pada *tag* RFID adalah data sidik jari yang di enkripsi (*chipertexs*).
2. Bedasarkan pengujian RMS yang telah dilakukan data sidik jari yang diamankan dalam tag RFID tidak dapat digunakan oleh penduduk yang tidak berhak. Disamping itu pada sistem ini dilakukan proses dekripsi untuk menampilkan data penduduk.

6. DAFTAR PUSTAKA

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi teori Analisis dan Implementasi.* Yogyakarta: Andi Offset

Batbold Toiruul,,KyungOh Lee, 2006*."An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems".* Sunmoon University http://paper.ijcsns.org/07_book/200609/200609C02.pdf [Diakses Mei 17 2011]

Munir, Rinaldi. 2004 . *Bahan Kuliah ke-13 IF5054 Kriptografi.* Bandung.

Putra, Darma. 2009. *Sistem Biometrika. Yogyakarta* : ANDI

Surian, D. 2006. *Algoritma Kriptografi AES Rijndael*. Teknik Elektro. TESLA. Vol. 8 No. 2 Hal. 97-101.

Mardhotillah, Rachma. 2011. Perancangan Sistem Keamanan Dalam Pentransmisian Data Dari Tag Menuju Reader Pada Rfid. http://digilib.its.ac.id/public/ITS-Undergraduate-13206-Paper.pdf Diakses tanggal 10 Januari 2011.

Virgan, R.Y. Agung, B.P. Agus S. *"Aplikasi Enkripsi dan Dekripsi Menggunakan Algoritma Rijndael".* Jurusan Teknik Elektro. Fakultas Teknik. Universitas Diponegoro.