DESAIN DAN IMPLEMENTASI APLIKASI SMS(SHORT MESSAGE SERVICE) PADA ANDROID MENGGUNAKAN ALGORITMA AES

DESIGN AND IMPLEMENTATION SMS(SHORT MESSAGE SERVICE) APPLICATIONS ON ANDROID USING AES ALGORITHM

, [2]**R.Rumani M**

[1,2,3]Jurusan Sistem Komputer – Universitas Telkom

Jl. Telekomunikasi, Dayeuhkolot, Bandung 40257, Indonesia
[2]rumani@telkomuniversity.ac.id

Abstrak

SMS(*Short Message Service*) adalah sebuah layanan yang di sediakan oleh operator untuk mengirimkan ataupun menerima sebuah pesan. SMS merupakan sebuah layanan yang praktis dan termasuk murah. Namun Jika pesan yang kita kirimkan merupakan pesan yang tidak boleh di lihat oleh orang lain maka akan timbul permasalahan keamanan data. Oleh karena itu di butuhkan kemanan pesan pada smartphone dengan menggunakan algoritma kriptografi maka pesan dapat di enkripsi dan di dekripsi dengan baik. Metode nya menggunakan android dalam pemrograman tersebut akan di gunakan algoritma AES.

Avalanche effect merupakan salah satu karakteristik yang menentukan baik atau tidak nya sebuah algoritma kriptografi dengan perubahan yang kecil pada plainteks akan menyebabkan perubahan yang signifikan terhadap *chippertext* yang di hasilkan. Nilai *avalanche effect* di katakan baik jika perubahan bit yang dihasilkan berkisar antara 45-60%. Hasil pengujian menunujukan bahwa nilai avalanche effect dari algoritma AES berkisar antara 45-60%. Dengan nilai tersebut akan membuat perbedaan yang cukup sulit untuk kriptanalis melakukan serangan.

Kata kunci: *sms, android, enkripsi, dekripsi, AES*

Abstract

SMS (Short Message Service) is a service provided by the operator to transmit or receive a message. SMS is a service that is practical and includes cheap. But if the message that we send a message that should not be seen by other people then there will be problems of data security.Therefore in need security message on the smartphone by using cryptographic algorithms then the message can be encrypted and decrypted properly. Her method uses Android in the programming will be in use algorithm aes.

Avalanche effect is one of the characteristics that determine whether or not its a cryptographic algorithm with a small change in the plaintext will cause significant changes to chippertext that produced . Avalanche effect on the value of said well if changes resulting bits ranging between 45-60 % . The test results menunujukan that the avalanche effect of AES algorithm ranged between 45-60 % . With this value will make the difference that is quite difficult to carry out an attack cryptanalyst .

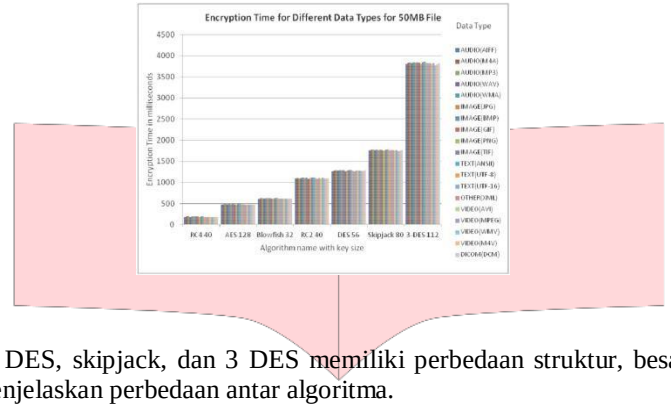
Keywords: sms, android, encryption, decryption, AES

1. PENDAHULUAN

1.1 Latar Belakang

Short Massage Service atau di singkat sms merupakan sebuah layanan dasar telekomunikasi seluler yang tersedia untuk jaringan gsm maupun cdma. Sebagai layanan dasar sms dapat di gunakan di semua jenis handphone.
Android merupakan sebuah sistem operasi yang sedang berkembang pesat. Dengan banyak nya fitur dan kemampuan yang terdapat pada android membuat sistem operasi ini sangat di minati masyarakat. Dengan banyak nya minat masyarakat terhadap android maka keamanan dalam melakukan pengiriman dan penerimaan pesan sangat di perlukan.

Kemanan dari sebuah pesan sangat di perlukan, karena tidak jarang orang-orang mengirimkan pesan-pesan yang sebenarnya tidak boleh di ketahui oleh orang lain. Oleh karena itu maka di perlukan sebuah aplikasi untuk dapat membuat aman isi dari pesan-pesan tersebut.Aplikasi tersebut harus mampu mengkodekan pesan yang asli agar menjadi sebuah pesan yang tidak dapat terbaca oleh orang lain tetapi hanya bisa di baca oleh orang yang di tuju. Untuk membuat aplikasi tersebut maka di gunakan sebuah algoritma yaitu algoritma AES.
Di bandingkan dengan algoritma blowfish, RC2, DES, skipjack, dan 3- DES algoritma AES memiliki waktu enkripsi yang cukup cepat. Di uji dengan cara mengenkripsi file dengan format text,image,audio dan video yang memiliki ukuran 50 mb, AES menjadi algoritma tercepat dalam melakukan enkripsi dapat di lihat pada tabel di bawah ini .



Algoritma blowfish, RC2, DES, skipjack, dan 3 DES memiliki perbedaan struktur, besar kunci dan ronde yang di lalui, berikut tabel yang menjelaskan perbedaan antar algoritma.

Tabel 1.1 Perbandingan Algoritma Kriptografi

Algorithm Name	Structure	Key Size (In bits)	Rounds	Cipher Type
AES	Substitution-permutation network	128, 192, 256	10, 12, 14	Block
DES	Balanced Feistel network	56	16	Block
Triple DES	Feistel network	112, 168	48	Block
RC2	Source-heavy Feistel network	40 to 1024	18	Block
Blowfish	Feistel network	32 to 448	16	Block
Skipjack	Unbalanced Feistel network	80	32	Block
RC4	----	40 to 2048	256	Stream

1.2 Rumusan Masalah

Rumusan masalah yang terdapat dalam penelitian ini adalah bagaimana cara *User* mengamankan pesan yang akan di kirim kepada orang lain agar tidak dapat di baca oleh orang lain. Dengan membuat sebuah aplikasi *mobile* pada perangkat *android*. Serta cara merancang desain aplikasi *mobile* tersebut beserta fitur-fiturnya sehingga dapat mengamankan pesan yang akan di kirim.

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian Tugas Akhir ini adalah memudahkan *User untuk* mengamankan pesan yang akan di kirim kepada orang lain , dengan membuat aplikasi *mobile* pada perangkat *android* sehingga pengguna dapat mengirimkan pesan yang dengan aman dan tidak dapat di baca oleh orang lain yang tidak berhak.

1.4 Batasan Masalah

Agar tidak terjadi kesalahan persepsi dan tidak meluasnya pokok bahasan, maka terdapat batasan-batasan masalah sebagai berikut :

1. Aplikasi ini diimplementasikan pada perangkat *android*.
2. Aplikasi *mobile* di buat menggunakan bahasa pemrograman Java dengan bantuan Android Software Development Kit (SDK).
3. Fitur yang di tampilkan adalah untuk menyandikan pesan yang di kirim.
4. Menggunakan algoritma AES.
5. Parameter yang dianalisis dari hasil implementasi adalah analisis sistem pada aplikasi dan analisis pemakaian aplikasi oleh pengguna.

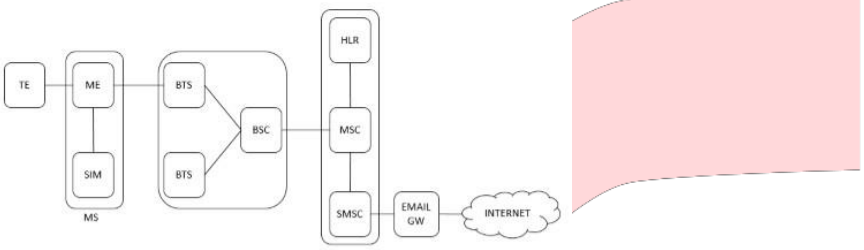
2. DASAR TEORI

2.1 SMS (*Short Message Service*)[7]

Short Message Service (SMS) merupakan salah satu fasilitas dari teknologi global system for communication(GSM) yang memungkinkan mengirim dan menerima pesan-pesan singkat berupa teks dengan kapasitas maksimal 160 karakter dari Mobile Station (MS). Kapasitas maksimal ini tergantung dari alphabet yang di gunakan, untuk alphabet latin maksimal 160 karakter , dan untuk non latin seperti alphabet arab atau china maksimal 70 karakter.

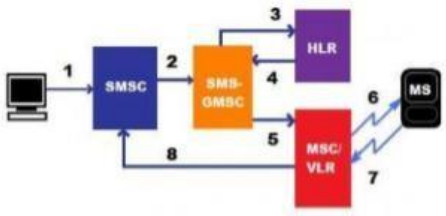
Dibawah ini menunjukan arsitektur dari SMS yang di integrasikan dengan jaringan GSM. Ada tiga elemen tambahan yaitu short message entity (SME), Short Message Service Center(SMSC) dan email gateway.

- Terminal Equipment (TE) merupakan perangkat yang di gunakan seperti hp yang terhubung dengan ME
- Mobile Equipment (ME) terdiri dari pemancar radio, display dan DSP
- Subscribe Identity Module (SIM) berfungsi untuk mengidentifikasi user pada jaringan



Gambar 2.1 Arsitektur SMS yang terintegrasi dengan jaringan GSM[1]

- Base Transceiver Station (BTS) terdiri dari pemancar radio untuk berkomunikasi dengan MS
- Base Station Controler (BSC) berfungsi untuk mengatur radio resources untuk satu atau lebih BTS
- Home Location Register (HLR) merupakan database yang memiliki data pelanggan tetap
- Mobile Switching Center (MSC) melaksanakan fungsi seperti registrasi, authentication, update lokasi.
- SMS Center (SMSC) mengatur proses pengiriman dan pemerimaan pesan dari dan atau menuju SME sesuai dengan proses store and forward
- Email gateway, sebuah gateway yang menghubungkan antara email dan sms pada intenet.



Gambar 2.2 Diagram alir SMS[1]

Diagram alir SMS mobile sebagai berikut

1. ME mengirim pesan ke SMSC
2. SMSC mengirimka pesan ke SMS-GMSC
3. SMS-GMSC menghubungi HLR untuk informasi routing
4. HLR membalas informasi routing ke SMS-GMSC
5. SMS-GMSC meneruskan pesan ke MSC/VLR
6. MS di-paging dan koneksi terbentuk antara MS dan network, sebagaimana dalam setup panggilan normal. (dengan demikian posisi MS di ketahui dan apakahMS boleh berada dalam network/proses otentikasi)
7. Jika otentikasi berhasil,MSC/VLR mengirim pesan tersebut ke MS
8. Jika pengiriman berhasil, delivery report di kirim dari MSC/VLR ke SMSC. Namun jika tidak, MSC/VLR akan menginformasikan ke HLR dan failure report di kirim ke SMS-C. pada kasus pengiriman yang gagal HLR dan VLR akan mendapat informasi “Message Waiting” yang menunjukan ada pesan di SMSC yang menunggu untuk di kirimkam ke MS. Informasi di HLR terdiri dari list SMSC pengiriman pesan, sedangkan

di VLR terdapat “flag”yang menunjukan apakah list pesan dalam keadaan kosong atau tidak. Jika MS available dan siap menerima pesan maka,HLR akan memberi tahu SMSC.

2.2 Android[4]

Android adalah sebuah sistem operasi untuk perangkat mobile berbasis linux yang mencakup sistem operasi, middleware dan aplikasi. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka. Awal nya google Inc. membeli android Inc. yang merupakan penatang baru yang membuat piranti lunak untuk ponsel/smartphone. Kemudian untuk mengembangkan android, di bentuklah Open Handset Alliance, konsorium dari 34 perusahaan peranti keras, peranti lunak dan telekomunikasi termasuk google, HTC, Intel, Motorola, Qualcomm, T-mobile, dan Nividia.

Android merupakan generasi baru platform mobile, platformyang memberikan pengembang untuk melakukan pengembangan sesuai dengan yang di harapkan nya. System operasi yang mendasari android di lisensikan di bawah GNU, General Public Lisensi Versi 2 (GPLv2), yang sering di kenal dengan istilah “copyleft” lisensi dimana setia perbaikan pihak ketiga harus terus jatuh di bawah terms . android di distribusikan di bawah lisensi Apache Software (ASL/Apache2), yang memungkinkan untuk distribusi kedua dan seterusnya.

Pengembang memiliki beberapa pilihan ketika membuat aplikasi yang berbasis android. Kebanyakan pengembang menggunakan eclipse yang tersedia secara bebas untuk merancang dan mengembangkan aplikasi android. Eclipse adalah Ide yang paling popular untuk pengembangan android, karena memiliki android plug-in yang tersedia untuk memfasilitasi pengembangan android. Selain itu eclipse juga mendapat dukungan langsung dari google untuk menjadi IDE pengmbangan aplikasi android, ini terbukti dengan adanya penambahan plugins untuk eclipse untuk membuat project android dimana source software langsung dari situs resminya google. Tetapi hal di atas tidak menutup kemungkinan untuk menggunakan IDE yang lain seperti Netbeans untuk melakukan pengembangan android.

2.3 Kriptografi [3]

Kriptografi, di lihat dari dua kata utama penyusunnya, yaitu crypto (rahasia) dan graphy (tulisan/pesan), maka dapat di artikan bahwa cryptography (kriptografi) merupakan sebuah bidang ilmu computer dan seni berbasiskan computer untuk dapat merahasiakan dan menjaga pesan atau tulisan agar tetap aman. Ada empat buah istilah dalam dunia kriptografi yaitu Cryptographer, Cryptanalyst, Cryptanalysis, dan Cryptologi. Cryptographer adalah orang atau pelaku yang melakukan kegiatan kriptografi atau berkecimpung di bidang kriptografi. Cryptanalyst adalah orang atau pelaku yang melakukan kegiatan cryptanalysis, termasuk juga yang menjadi pakar di bidang cryptanalysis. Cryptanalysis adalah sub bagian di dalam kriptografi yang khusus mempelajari tentang cipher text dari berbagai sudut pandang penyusunan dan pemecahan nya tanpa harus menggunakan kunci. Cryptologi adalah cabang ilmu computer, jaringan computer, dan kemanan computer/ jaringan computer yang khusus mempelajari mengenai teknis di dalam kriptografi.

2.4 *AES*[3]

AES merupakan sistem penyandian blok yang bersifat non-Feistel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Kunci AES dapat memiliki panjang kunci bit 128, 192 dan 256 bit. Penyandian AES menggunakan proses yang berulang yang di sebut dengan ronde. Jumlah ronde yang di gunakan oleh AES tergantung dengan panjang kunci yang di gunakan. Setiap ronde membutuhkan kunci ronde dan masukan dari ronde berikut nya . kunci ronde di bangkitkan berdasarkan kunci yang di berikan. Relasi antara jumlah ronde dan panjang kunci di berikan oleh

Panjang Kunci AES (bit)	Jumlah Ronde (Nr)
128	10
192	12
256	14

Tabel 2.4.1 hubungan antara jumlah ronde dan panjang kunci AES [3]

2.5 Struktur enkripsi AES[3]

Proses di dalam AES merupakan transformasi terhadap state. Sebuah teks asli dalam blok (128 bit) terlebih dahulu di organisir sebagai state. Enkripsi AES adalah trasformasi state secara berulang dalam beberapa ronde. State yang menjadi keluaran ronde k menjadi masukan untuk ronde ke- k+1.

Pada awal nya teks asli di reorganisasi sebagai sebuah state. kemudian sebelum ronde 1 di mulai blok teks asli dicampur dengan kunci ronde ke-0 (transformasi ini di sebut dengan AddRoundKey). Setelah itu ronde ke-1 sampai

dengan ronde ke-(Nr – 1) dengan Nr adalah jumlah ronde menggunakan 4 jenis transformasi yaitu SubBytes, ShiftRows, MixColumns dan AddRoundKey. Pada ronde terakhir, yaitu ronde ke-Nr di lakukan transformasi serupa dengan ronde lain namun tanpa transformasi MixColumn.

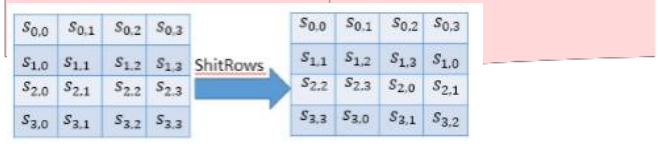
2.6 **Subbytes**[3]

Aes menggunakan substitusi nonlinear pada ukuran byte yang di sebut SubBytes. Setiap elemen pada state dari elemen sampai dengan di kenakan transformasi SubBytes.

Transformasi SubBytes menggunakan table substitusi, yaitu dengan cara menginterpretasikan byte masukan sebagai dua bilangan heksadesimal, kemudian digit kiri menunjukan indeks baris dan digit kanan menunjukan indeks kolom di table substitusi. Nilai byte pada table substitusi yang di rujuk oleh indeks baris dan kolom menjadi nilai yang mensubstitusi .

2.7 **Shiftrows**[3]

Selain menggunakan substitusi untuk mengganti nilai pada elemen state, AES menggunakan permutasi pada state. Transformasi permutasi pada state di sebut dengan transformasi ShiftRows. ShiftRows di lakukan dengan menjalan operasi circular shift left sebanyak I pada baris ke-I pada state.

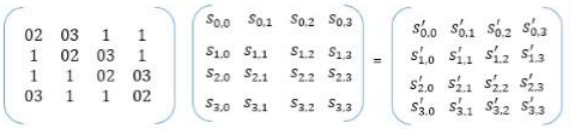


Gambar 2.4.4 Proses ShiftRows[3]

Transformasi ShiftRows merupakan jenis transformasi permutasi, yaitu pengubahan posisi elemen pada state tanpa mengubah nilai nya.

2.8 **Mixcolumn**[3]

Tujuan transformasi MixColumn adalah mencampur nilai kolom kolom pada state pada satu elemen pada state keluaran. Untuk melakukan pencampuran itu, transformasi MixColumn menggunakan operasi perkalian matriks dengan operasi perkalian dan penjumlahan menggunakan operator pada GF( ) dengan irreduciable polynomial (+ + +x+1).



Gambar 2.4.5 Transformasi MixColumns[3]

Pada gambar 2.4.5, state S adalah masukan transformasi MixColumn dan state adalah keluaran transformasi MixColumn. Representasikan biner elemen S sebagai polynomial lalu lakukan perkalian vector antara baris ke-i pada konstan dan kolom ke-j pada S. perkalian dan penjumlahan menggunakan GF( ).

2.9 **Addroundkey**[3]

Transformasi keempat yang di gunakan pada penyandian AES adalah transformasi AddRoundKey. Transformasi AddRoundKey mencampur sebuah state masukan dengan kunci ronde dengan operasi eksklusif OR ( ). Setiap elemen pada state masukan yang merupakan sebuah byte di kenakan operasi eksklusif OR dengan byte pada posisi yang sama di kunci ronde (Kunci ronde di representasikan sebagai state).Transformasi AddroundKey merupakan transformasi yang bersifat self invers, yaitu transformasi invers sama dengan transformasi aslinya asalkan menggunakan kunci ronde yang sama.

3. PERANCANGAN SISTEM

3.1 Deskripsi Sistem

Aplikasi ini memiliki fungsi utama untuk mengirim pesan teks dalam bentuk terenkripsi kepada penerima dan pada penerima di lakukan dekripsi sehingga pesan teks dapat sampai dengan aman dan dapat di baca dengan baik oleh penerima.Untuk menggunkan aplikasi ini, hal pertama yang harus di lakukan adalah melakukan registrasi

untuk mendapatkan username dan password. Setelah itu masuk kedalam aplikasi dengan username dan password yang sebelum nya telah di daftarkan. Setelah masuk kedalam menu maka pilih menu tulis pesan, isi nomer yang akn di tuju setelah menggklik tombol kirim maka pesan tersebut akan terkirim ke server untuk di enkripsi menggunakan algoritma AES setelah pesan terenkripsi baru kemudian pesan tersebut akan di kirim ke penerima.Untuk memudahkan proses perancangan dan implementasi, diperlukan flowchart. Flowchart yang dibuat akan menjelaskan garis besar proses yang dilakukan saat pelaksanaan tugas akhir

3.2 Perancangan Desain Antar Muka

Dalam perancangan aplikasi dibutuhkan suatu antarmuka (*interface*). Perancangan antarmuka terdiri atas tampilan menu utama, sub-menu, dan tampilan ketika suatu aksi (*action*) dijalankan

1. Antarmuka Memulai Aplikasi

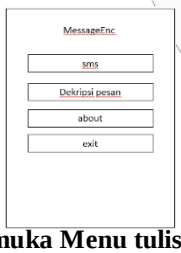
Rancangan antarmuka ketika aplikasi pertama kali dibuka oleh *user* akan langsung menuju menu utama. Berikut tampilan dari rancangan antarmuka untuk menu utama aplikasi :

2. Antarmuka Menu "register"

Menu register berfungsi untuk melakukan registrasi user. Menu ini berisi user name, password, key dan phone

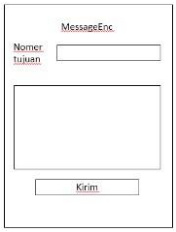
3. Antarmuka Menu utama

Menu utama ini berisi tentang menu-menu yang dapat di akses dalam aplikasi ini antara lain sms untuk menulis sms, dekripsi sms untuk mendekripsi pesan yang masuk, about berisi tentang aplikasi dan exit untuk keluar aplikasi.



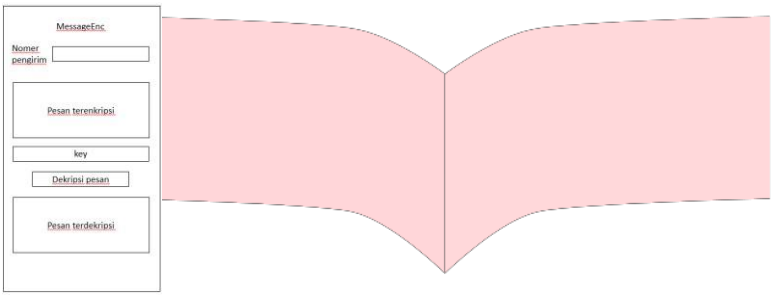
4. Antarmuka Menu tulis sms

Pada menu tulis SMS ini berfungsi untuk menulis pesan yang akan kita kirim dengan memasukan no tujuan dan pesan yang akan di kirim



5. Antarmuka menu dekripsi

Menu dekripsi ini berfungsi untuk mendekripsi pesan yang di terima dengan cara mengklik tombol key lalu memilih siapa yang telah mengirimkan pesan tersebut sehingga nanti pesan dapat terdekripsi dengan baik dan dapat di baca kembali.

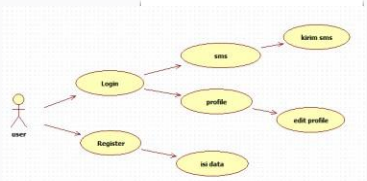


3.3 Perancangan Aplikasi

Perancangan aplikasi ini digunakan pemodelan menggunakan Unified Model Language (UML). UML dalam pembuatan aplikasi ini terdiri atas use case diagram, activity diagram dan sequence diagram.

3.3.1 usecase diagram

Use case merupakan gambaran scenario dari interaksi antara pengguna (user) dengan aplikasi . sebuah diagram use case menggambarkan hubungan antara pengguna (user) dan kegiatan yang akan dilakukannya terhadap aplikasi. Use case diagram aplikasi secara umum dapat dilihat pada gambar berikut :



4. Pembahasan

4.1 Pengujian

Pada aplikasi ini dilakukan dua buah jenis pengujian, yaitu pengujian secara fungsional (*alpha* dan *beta*) dan pengujian performansi aplikasi. Metode yang digunakan dalam pengujian ini adalah pengujian *black box* yang berfokus pada persyaratan fungsional dari perangkat lunak yang dibangun.

4.1.1 Pengujian alpha

Pengujian perangkat lunak ini berikut menggunakan data uji berdasarkan data dari masing-masing data. Rencana selengkapnya dapat dilihat pada tabel berikut :

Tabel 1.4.1 Rencana Pengujian

Kelas uji	Butir uji	Jenis pengujian
Menu utama	Menampilkan menu utama	*Black Box*
Menu registrasi	Menampilkan menu registrasi	*Black Box*
Login	Masuk kedalam aplikasi dengan berhasil login	*Black Box*
Menu registrasi	Masukan data kedalam data base	*Black Box*
Menu sms	Melakukan pengiriman pesan	*Black Box*
Menu dekripsi	Melakukan dekripsi pesan	*Black Box*

4.1.2 Pengujian beta

Pengujian beta merupakan pengujian yang dilakukan secara objektif dimana diuji secara langsung ke lapangan yaitu *user*. Dari hasil kuesioner tersebut akan dilakukan perhitungan untuk dapat diambil kesimpulannya terhadap penilaian dari aplikasi.

Analisa Fungsi Aplikasi :

1. Bagaimana dengan tingkat kebutuhan aplikasi ini dalam mencari mengamankan pesan?

Gambar 1.4.1 Diagram Tingkat Kebutuhan Aplikasi

Dari tabel diatas dapat dilihat hasil perhitungan kuisioner di dapatkan 75% menyatakan bahwa tingkat kebutuhan aplikasi ini dalam mengamankan pesan user.

4.1.3 Pengujian *avalanche effect*

Avalanche effect adalah perubahan satu bit pada plaintext atau key yang menyebabkan perubahan yang signifikan terhadap chiphertext suatu algoritma akan di katakan memiliki nilai AE yang baik jika perubahan satu bit saja pada input menghasilkan perubahan sekitar setengah jumlah bit pada output nya. Salah satu fungsi dari AE adalah untuk melihat tingkat keamanan suatu algoritma kriptografi.

Tabel 4.5.1.1 pengujian plaintext

no	plaintext	key	chiphertext	jumlah	
				plaintext	chiphertext
1	tugasakhir1	826501	TRs5j3mlSxubh8a8lhoVzQ==	11	24
2	tugasakhir2	826501	CtFhS54gwFM2DRk2gr6Ebw==	11	24
3	enkripsi1	826501	8S9gJrE06pMnO1Q4sK4nGA==	11	24
4	enkripsi2	826501	hSZW7RD15uz6cNKHbjVgBw==	11	24
5	dekripsi	826501	7DzUgJXYAYekX8HcChTPvQ==	8	24
6	dekripsj	826501	c9KByPHqAnov7e9w2zNNRQ==	8	24
7	ALGORITMA	826501	7g8pF5hcyHlJbQN5py2dlg==	9	24
8	ALGORITMB	826501	U1wUE+q3RkEtwhr7Jf/5mw==	9	24
9	ANALISIS1	826501	lGjW+H46GOUa6iJFZqQsMA==	9	24
10	ANALISIS2	826501	C0GhZbTM/E0yygjWtYcf2w==	9	24

Dari hasil pengujian pada tabel 4.5.1.1 di atas perubahan 1 byte pada plaintext dengan menggunakan kunci yang sama menghasilkan perubahan yang cukup banyak pada chipher text yang di hasilkan. Jika di hitung nilai avalanche effect nya akan menghasilkan nilai berikut

Tabel 4.5.1.2 Pengujian avalanche effect

plaintext	chiphertext	avalanche effect
tugasakhir	eJT7mKxkdlJZgcthjgm+mA==	0,442(85)
tugasakhis	flvQYYW4kRxp9b+nTZWJOg==	
tugasakhir1	TRs5j3mlSxubh8a8lhoVzQ==	0,432(80)
tugasakhir2	CtFhS54gwFM2DRk2gr6Ebw==	
dekripsi	7DzUgJXYAYekX8HcChTPvQ==	0,468(90)
dekripsj	c9KByPHqAnov7e9w2zNNRQ==	

Setelah di hitung menggunakan persamaan 4.5.1.1 di dapatkan hasil avalanche effect 0,442 untuk percobaan pertama 0,432 untuk percobaan kedua dan 0,468 untuk percobaan ketiga. Avalanche effect merupakan salah satu karakteristik terpenting dalam sebuah algoritma enkripsi. Efek ini dapat di lihat dengan cara mengubah 1 bit pada plaintext kemudian kita lihat pada chipher text maka akan berubah setidaknya setengah dari total bit dalam chiphertext. Salah satu dari tujuan ada nya tes avalanche effect ini adalah bahwa hanya dengan mengubah satu bit pada plaintext maka aka nada perubahan besar pada chiphertext sehingga lebih sulit untuk melakukan analisis chiphertext.

5 . Kesimpulan dan saran

5.1 Kesimpulan

Berdasarkan analisa pengujian *alpha* dan *beta* pada BAB IV dapat ditarik beberapa kesimpulan sebagai berikut :

1. Aplikasi ini sudah dapat digunakan oleh pengguna dalam mengamankan pesan. Yang ditunjukkan dengan 55 % dari total responden yang menyatakan aplikasi ini berfungsi dengan baik dan dari hasil pengamatan pengujian fungsi menu yang sesuai harapan
2. Hasil avalanche effect dari percobaan yang sudah di lakukan membuktikan bahwa perubahan 1 bit dari plaintext akan menghasilkan paling tidak setengah perbedaan pada chipher text hal ini menunjukan bahwa algoritma ini baik.
3. Tingkat keberhasilan enkripsi dan dekripsi menggunakan algoritma AES adalah 100%
4. Aplikasi berfungsi dengan baik mampu mengamankan pesan terbukti dapat memudahkan user untuk melakukan enkripsi dan dekripsi pesan
5. Algoritma AES berhasil di terapkan pada aplikasi messageesc

5.2 Saran

Saran untuk pengembangan aplikasi:

1. Interface aplikasi di buat lebih baik dan lebih lengkap lagi agar memudahkan user dalam menggunakan nya
2. Untuk dekripsi pesan agar dapat di lakukan langsung tanpa menghapus username pengirim.
3. Penambahan fitur-fitur yan lebih baik lagi

DAFTAR PUSTAKA

[1] Hidayatullah, priyanto dan Jauhari khairul kawistara.(2014).Pemrograman Web.Informatika Bandung.
[2] Pratama i putu agus(2014).Handbook Jaringan Komputer teori dan praktik berbasiskan open source.Informatika Bandung.
[3] Sadikin rifki.(2012).Kriptografi untuk keamanan jaringan dan implementasinya dalam bahasa java.ANDI
[4] Safaat Nazrudin.(2014).Android Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android.Informatika Bandung.
[5] Satyaputra Alfa, eva maulina aritonang.(2014).Begining Android Programming with ADT Bundle.PT Elex Media Komputindo.
[6] Wahana computer, penerbit andi.(2013).Step by Step Menjadi Programmer Android.C.V ANDI OFFSET
[7] Wibisono gunawan, uke kurniawan usman dan gunadi dwi hantoro.(2008).Konsep Teknologi Seluler.Informatika Bandung.
[8] Winarno edy, ali zaki, smitdev community.(2011).Membuat sendiri aplikasi android untuk pemula.PT Elex Media Komputindo.
[9] Winarno edy, ali zaki, smitdev community.(2014).Pemrograman Web Berbasis HTML 5, PHP dan JavaScript.PT Elex Media Komputindo.
[10] Masram ranjeet, Jibi abraham, Rajni moona, Vivex shahare, Juli 2014, “Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based on Various FileFeatures”. Volume 6, no.4, http://airccse.org/journal/nsa/6414nsa04.pdf, 29 juni 2015.