APLIKASI SMS KRIPTOGRAFI MENGGUNAKAN METODE AES BERBASIS ANDROID

Jainal Ibrahim Hanafi, Andi Patombongi.
STMIK Catur Sakti Kendari,
Jl Drs. Abdullah Silondae No. 109 , (0401)327275
tomfiq@gmail.com.

Layanan pesan singkat atau SMS merupakan salah satu komunikasi , ponsel yang banyak diminati di kalangan masyarakat karena biaya yang relatif rendah . Namun seiring dengan perkembangan teknologi yang semakin canggih menimbulkan pertanyaan tentang keamanan informasi yang dikirimkan melalui SMS . Untuk itu penulis mencoba untuk membuat aplikasi sms menggunakan ilmu kriptografi . Algoritma kriptografi dan berkembang cukup pesat , salah satunya adalah (Advanced Encryption Standard) AES . Algoritma ini menggunakan empat transformasi untuk mengenkripsi yang SubBytes ( ) , ShiftRows ( ) , MixColoums ( ) , dan AddRoundKeys ( ) . Teknik keempat adalah apa yang membuat AES sebagai agoritma terbaik di seluruh dunia dalam kriptografi kunci simetris.

***Kata Kunci -- sms, android, kriptografi, aes*.**

I. PENDAHULUAN

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 bisa mengelak (Non- Repudiation).(Ariyus Dony, 2008).

Algoritma AES (Advanced encryption standar) merupakan algoritma kriptografi simetrik yang beroperasi dalam mode penyandi blok (block cipher) yang memproses blok data 128-bit dengan panjang kunci 128-bit (AES- 128), 192-bit (AES-192), atau 256-bit (AES-256). AES juga merupakan algoritma yang sangat terkenal di Amerika dan pernah menjadi keamanan dasar yang digunakan di seluruh dunia dalam kriptografi kunci simetrik. Selain keunggulan yang telah disebutkan, Algoritma AES juga dirancang untuk memiliki properti ketahanan terhadap semua jenis serangan yang telah diketahui, kesederhanaan rancangan dan kekompokan kode serta kecepatan koputasi pada berbagai platform.

Berdasarkan uraian diatas, maka penulis tertarik untuk melakukan sebuah penelitian dengan judul Aplikasi SMS Kriptografi Menggunakan Metode AES Berbasis Android.

Yang menjadi tujuan penelitian ini adalah menghasilkan suatu aplikasi pada telepon seluler berbasis android yang dapat mengenkripsi pesan SMS dengan menggunakan metode AES agar pesan tersebut tidak dapat diketahui oleh orang lain.

Agar pembahasan penulisan ini tidak melebar dan keluar dari latar belakang penelitian, maka penulis hanya membatasi penelitian diantaranya adalah (1) Enkripsi yang dilakukan hanya berupa pesan text data SMS; (2) Jenis perangkat mobile harus beroperasi sistem android; (3) Dua belah pihak pengguna harus sama – sama menggunakan aplikasi ini; (4) Tehnik mengamankan pesan menggunakan tehnik ilmu kriptografi dengan menggunakan metode AES dengan panjang kunci 128 *bit;* (5) Bahasa pemograman yang digunakan adalah java Android

II. LANDASAN TEORI

2.1 Kriptografi

Kata kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata *Cryptos* yang artinya tersembunyi dan *Graphein* yang artinya menulis. Kriptografi dapat diartikan sebagai suatu ilmu ataupun seni yang mempelajari bagaimana sebuah data dikonversi ke bentuk tertentu yang sulit untuk dimengerti (Bruce Schneier, 1996).

Menurut Dony Ariyus, (2006) kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Menurut Rinaldi Munir (2006) Kriptografi adalah

ilmu dan seni yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentifikasi. Kata seni ini berasal dari fakta sejarah kriptografi, bahwa setiap orang mempunyai cara yang unik untuk merahasiakan pesan. Cara-cara unik mungkin berbeda-beda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia mempunyai nilai estetika tersendiri. Didalam kriptografi ada beberapa istilah yang sering digunakan, yaitu:

TIPE	PANJANG KUNCI (Nk)	UKURAN BLOK (Nb)	JUMLAH PUTARAN (Nr)
AES - 128	4	4	10
AES - 192	6	4	12
AES - 256	8	4	14

a. *Plaintext*. *Plaintext* adalah data atau informasi yang dapat dibaca dan dimengerti maknanya dapat berupa data atau informasi yang dikirim melalui kurir, saluran telekomunikasi dan sebagainya atau yang disimpan di dalam media perekman. Pesan yang tersimpan tidak hanya berupa teks tetapi juga dapat berbentuk gambar, suara, video atau lainnya
b. Pengirim dan penerima. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan. Entitas disini dapat berupa orang, mesin (komputer), kartu kredit, dan sebagainya.
c. Enkripsi dan dekripsi. Proses menyendikan *plainteks* menjadi *chiperteks* disebut enkripsi, sedangkan proses mengembalikan *cipherteks* menjadi *plainteks* semula dinamakan dekripsi. Enkripsi dan dekripsi dapat diterapkan baik pada pesan yang dikirm maupun pada pesan yang tersimpan. Berikut gambar aliran enkripsi dan dekripsi
d. *Cipher* dan kunci. Algoritma kriptografi disebut juga *cipher* yaitu aturan untuk *enchipering* dan *dechipering*, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi

2.2 AES (Advanced Encryption Standard)

Dalam kriptografi, *Advanced Encryption Standard* (AES) merupakan standar enkripsi dengan kunci simetris yang diadopsi oleh pemerintah Amerika Serikat. Standar ini terdiri atas 3 blok cipher, yaitu AES128, AES192 dan AES 256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Masing-masing cipher memiliki ukuran 128 bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit. AES telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya, Data Encryption Standard (DES). Alasan utama terpilihnya AES ini bukan karna algoritmanya yang paling aman dari *MARS*, *RC6*, *Serpent*, *Twofish* dan yang lainya, tetapi AES memiliki keseimbangan antara keamanan serta fleksibelitas dalam berbagai platform *software* dan *hardware*. (Dony Ariyus, 2005).

AES mendukung panjang kunci 128 bit sampai 256 bit Panjang kunci dan ukuran Blok dapat dipilih secara independen dan setiap blok dienkripsi sejumlah putaran tertentu.

Tabel 1. Jumlah putaran pengoperasian AES 128

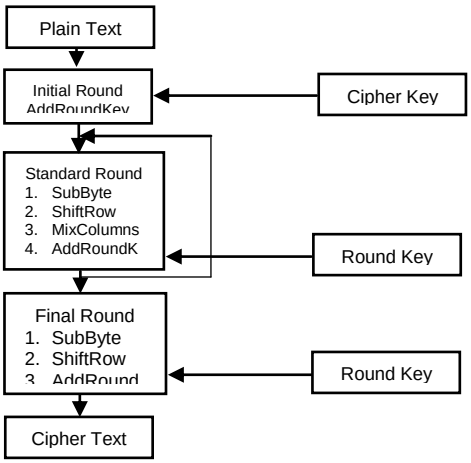
AES mempunyai panjang kunci paling sedikit 128 bit, maka AES tahan terhadap serangan exhaustive key search dengan teknologi saat ini. Dengan panjang kunci 128 bit, maka terdapat sebanyak: 2128 = 3,4 × 1038 kemungkinan kunci. Jadi Jika digunakan komputer tercepat yang dapat mencoba 1 juta kunci setiap detik, maka akan dibutuhkan waktu 5,4 × 1024 tahun untuk mencoba seluruh kemungkinan kunci. Jika digunakan komputer tercepat yang dapat mencoba 1 juta kunci setiap milidetik, maka akan dibutuhkan waktu 5,4 × 1018 tahun untuk mencoba seluruh kemungkinan kunci. (Rinaldi Munir, 2006).

2.3 Enkripsi AES 128

Garis besar enkripsi Algoritma AES yang beroperasi pada Blok 128-bit dengan kunci 128-bit adalah sebagai berikut: (Rinaldi Munir, 2006).

a. *AddRoundKey*: melakukan X-or antara *state* awal (*plainteks*) dengan *cipher key*. Tahap ini disebut juga *initial round*.
b. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
    a. *SubBytes*: substitusi *byte* dengan menggunakan tabel substitusi (*S-box*).
    b. *ShiftRows*: pergeseran baris-baris *array state* secara wrapping
    c. *MixColumns*: mengacak data pada masing-masing kolom *array state*
    d. *AddRoundKey*: melakukan operasi X-or antara *state* sekarang dengan *round key*
c. Final round: proses untuk putaran terakhir:
    a. *SubBytes*
    b. *ShiftBytes*
    c. *AddRoundKey*

Proses enkripsi AES dapat dilihat pada Blok diagram pada Gambar 1. dengan Nr merupakan banyaknya putaran yang dilakukan dengan Nn adalah putaran ke-n

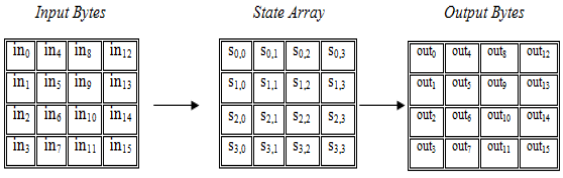


Gambar 1. Blok Diagram Proses Enkripsi AES

Algoritma AES mempunyai 3 parameter:

1. *Plaintext*: array yang berukuran 16-byte, yang berisi data masukan.
2. Ciphertext: array yang berukuran 16-byte, yang berisi hasil enkripsi.
3. *Key*: array yang berukuran 16-byte, yang berisi kunci ciphering (disebut juga cipher key).

Dengan 16 byte, maka baik Blok data dan kunci yang berukuran 128-bit dapat disimpan di dalam ketiga array tersebut (128 = 16 × 8). Selama kalkulasi plainteks menjadi cipherteks, status sekarang dari data disimpan di dalam array of bytes dua dimensi, state, yang berukuran NROWS × NCOLS. Untuk Blok data 128-bit, ukuran state adalah 4 × 4. Elemen array state diacu sebagai S[r,c], dengan $0 \leq r < 4$ dan $0 \leq c < Nb$ (Nb adalah panjang blok dibagi 32. Pada AES- 128, Nb = 128/32 = 4). Pada awal enkripsi, 16-byte data masukan, in_0, in_1, …, in_{15} disalin ke dalam array state (direalisasikan oleh fungsi CopyPlaintextToState (state, plaintext)) seperti diilustrasikan sebagai berikut:



Gambar 2.Ilustrasi Enkripsi AES

Operasi enkripsi/dekripsi dilakukan terhadap array S, dan keluarannya ditampung didalam array out. Skema penyalinan array masukan in ke array S:

S[r, c] in[r + 4c] untuk $0 \leq r < 4$ dan $0 \leq c < Nb$

Skema penyalinan array S ke array keluaran out:

out[r+4c] S[r, c] untuk $0 \leq r < 4$ dan $0 \leq c < Nb$

(Rinaldi Munir, 2006).

Karena terjadi beberapa tahap dalam proses enkripsi, maka diperlukan *subkeysubkey* yang akan dipakai pada tiap tahap. Pengembangan jumlah kunci yang akan dipakai diperlukan karena kebutuhan *subkeysubkey* yang akan dipakai dapat mencapai ribuan bit, sedangkan kunci yang disediakan secara *default* hanya 128-256 bit. Jumla total kunci yang diperlukan sebagai *subkey* adalah sebanyak *Nb(Nr+1)*, dimana *Nb* adalah besarnya blok data dalam satuan *word*. Sedangkan *Nr* adalah jumlah tahapan yang harus dilalui dalam satuan *word*. Sebagai contoh, bilamana digunakan 128 bit (4 word) blok data dan 128 bit (4 word) kunci maka akan dilakukan 10 kali proses (lihat Tabel 2.1). Dengan demikian dari rumus didapatkan 4(10+1)=44 word=1408 bit kunci. Untuk melakukan pengembangan jumlah kunci yang akan dipakai dari kunci utama maka dilakukan *key schedule*.

2.4 Dekripsi AES 128

Dekripsi AES merupakan kebalikan dari enkripsi AES. Algoritma dekripsi AES menggunakan transformasi invers semua transformasi yang digunakan pada algoritma enkripsi AES, yaitu: InvSubBytes, InvShiftRows, InvMixColumns. Sedangkan transformasi AddRoundKey merupakan transformasi bersifat self-invers dengan syarat menggunakan kunci yang sama.

Garis besar dekripsi algorima AES yang beroperasi pada blok 128-bit adalah sebagai berikut:

1. AddRoundKey : melakukan X-or antara *state awal* (*cipherteks*) dengan *cipher key*. Tahap ini disebut *initial round*
2. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah :
   a. *InvShiftRow* : pergeseran baris-baris *array state* secara *wrapping*
   b. *InvSubByte* : substitusi *byte* dengan menggunakan tabel substitusi *inverse* S-box
   c. *AddRoundKey* : melakukan operasi X-or antara *state* sekarang dengan *round key*
   d. *InvMixColumn* : mengacak data pada masing-masing kolom *array state*
3. Final Round : proses untuk putaran terakhir :
   a. *InvShiftRow*
   b. *Inv SubByte*
   c. *AddRoundKey*

2.5 Android

Menurut (Safaat, 2012) android adalah sebuah sistem operasi untuk perangakat mobile berbasis

Linux yang mencakup sistem operasi, middleware dan aplikasi.

Pada Juli 2005, Google bekerjasama dengan Android Inc, perusahaan yang berada di Palo Alto, California Amerika Serikat. Para pendiri Android Inc. bekerja pada Google, di antaranya Andy Rubin, Rich Miner, Nick Sears, dan Chris White. Saat itu banyak yang menganggap fungsi Android Inc. hanyalah sebagai perangkat lunak pada telepon seluler. Sejak saat itu muncul rumor bahwa Google hendak memasuki pasar telepon seluler. Di perusahaan Google, tim yang dipimpin Rubin bertugas mengembangkan program perangkat seluler yang didukung oleh kernel Linux. Hal ini menunjukkan indikasi bahwa Google sedang bersiap menghadapi persaingan dalam pasar telepon seluler.

Sekitar September 2007 sebuah studi melaporkan bahwa Google mengajukan hak paten aplikasi telepon seluler (akhirnya Google mengenalkan Nexus One, salah satu jenis telepon pintar GSM yang menggunakan Android pada sistem operasinya. Telepon seluler ini diproduksi oleh HTC Corporation dan tersedia di pasaran pada 5 Januari 2010).

Pada 9 Desember 2008, diumumkan anggota baru yang bergabung dalam program kerja Android ARM Holdings, Atheros Communications, diproduksi oleh Asustek Computer Inc, Garmin Ltd, Softbank, Sony Ericsson, Toshiba Corp, dan Vodafone Group Plc. Seiring pembentukan Open Handset Alliance, OHA mengumumkan produk perdana mereka, Android, perangkat bergerak (mobile) yang merupakan modifikasi kernel Linux 2.6. Sejak Android dirilis telah dilakukan berbagai pembaruan berupa perbaikan bug dan penambahan fitur baru.

Telepon pertama yang memakai sistem operasi Android adalah HTC Dream, yang dirilis pada 22 Oktober 2008. Pada penghujung tahun 2009 diperkirakan di dunia ini paling sedikit terdapat 18 jenis telepon seluler yang menggunakan Android.

2.6 Android SDK

(Safaat, 2012) Android SDK (Software Development Kit) adalah tools API yang diperlukan untuk memulai mengembangkan aplikasi pada platform Android menggunakan bahasa pemrograman Java. Beberapa fitur-fitur Android yang paling penting adalah

7. Framework Aplikasi yang mendukung penggantian komponen dan reusable.
8. Mesin Virtual Dalvik berjalan diatas Linux kernel dan dioptimalkan untuk perangkat mobile.
9. Integrated browser berdasarkan open source engine WebKit.
10. Grafis yang dioptimalkan dan didukung oleh libraries grafis 2D, grafis 3D berdasarkan spesifikasi OpenGL ES 1,0 (Opsional akselerasi hardware).
11. Media support yang mendukung audio, video, dan gambar (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF), GSM Telephony (tergantung hardware).
12. Kamera, GPS, kompas, dan accelerometer (tergantung hardware).

Lingkungan Development yang lengkap dan kaya termasuk perangkat emulator, tools untuk debugger, profil dan kinerja memori dan plugin.

2.7 Android Virtual Device (AVD)

Android Virtual Device merupakan emulator untuk menjalankan aplikasi android, (http://developer.android.com/ di akses 20 Januari 2015).

Gambar. 1. Tampilan AVD

2.8 Android Studio

Android Studio merupakan salah satu IDE (Integrated Development Environment) untuk membuat Aplikasi Android, android studio adalah lingkungan pengembangan Android baru berdasarkan IntelliJ IDEA. Mirip dengan Eclipse dengan ADT Plugin, Android Studio menyediakan alat pengembang Android terintegrasi untuk pengembangan dan debugging. (http://developer.android.com/tools/studio/index.html diakses 5 Januari 2015)

Gambar. 2. Android Studio

2.9 Java

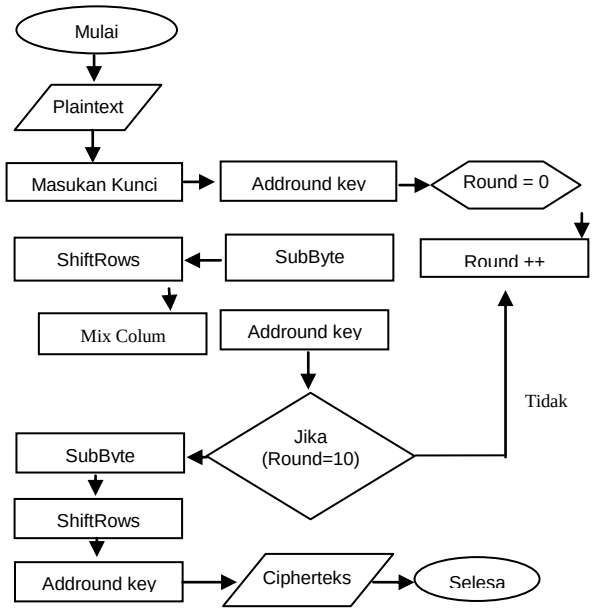
Java adalah bahasa pemrograman yang dapat dijalankan di berbagai komputer termasuk telepon genggam. Dikembangkan oleh Sun Microsystem dan diterbitkan tahun 1995. Keunggulan java yaitu Berbasis GUI , berorientasi objek, aplikasi web dan multiplatform. Platform Java terdiri dari kumpulan library, JVM, kelas-kelas loader yang dipaket dalam sebuah lingkungan rutin Java, dan sebuah c*ompiler*, *debugger* dan kakas lain yang dipaket dalam Java Development Kit (JDK).

Java adalah generasi yang sedang berkembang dari platform Java. Agar sebuah program Java dapat dijalankan, maka file dengan ekstensi .java harus dikompilasi menjadi filebytecode. Untuk menjalankan bytecode tersebut dibutuhkan JRE (Java Runtime Environment) yang memungkinkan pemakai untuk menejalankan program Java,hanya menjalankan, tidak untuk membuat kode baru lagi. JRE berisi JVM dan library Java yang digunakan. Platform Java memiliki tiga buah edisi yang berbeda, yaitu (1) Java2 Enterprise Edition (J2EE); (2) Java2 Standard Edition (J2SE); (3) Java2 Micro Edition (J2ME).

III. METODE PENELITIAN

3.1. Flowchart Enkripsi AES 128

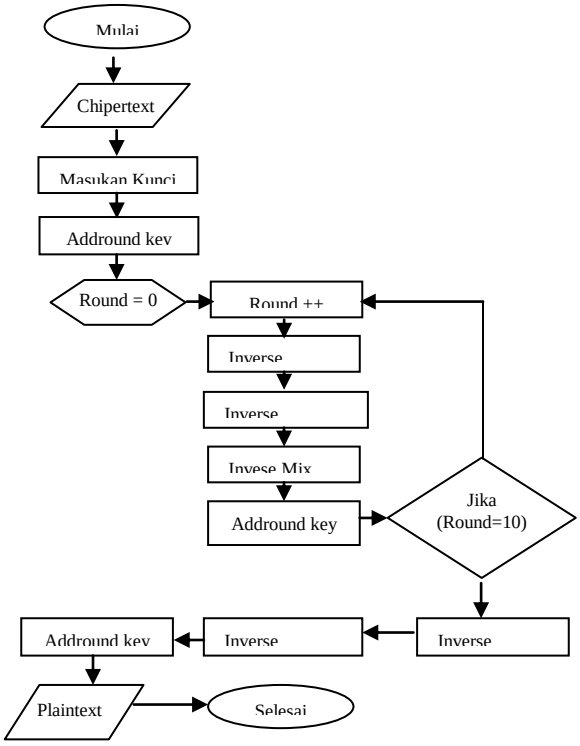
Enkripsi AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dikopikan ke dalam state akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak 10 Round. Proses ini dalam algoritma AES disebut sebagai round function. Round yangterakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns, Lowchart Enkripsi AES 128 bit terlihat pada Gambar 3.



Gambar 3. Flowchart Enkripsi AES 128 Bit

3.2. Flowchart Deskripsi AES 128

Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Algoritma dekripsi dapat dilihat pada Gambar 4.



Gambar 4. Flowchart Deskripsi AES 128 Bit

IV. HASIL DAN PEMBAHASAN

4.1 Transformasi Algoritma AES

AES menggunakan 4 jenis transformasi byte untuk mengenkripsi pesan yaitu SubByte, ShiftRows, MixColumns dan AddRoundKey. Kecuali tahap MixColumns, ketiga tahap lainnya akan diulang sebanyak 10 Round kecuali tahap MixColumns tidak akan dilakukan pada tahap terakhir. Sedangkan proses dekripsi, transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan InvAddRoundKey.

4.2 Implementasi

Aplikasi ini diimplementasikan dari desain dan kode berdasarkan rancangan bab sebelumnya. Aplikasi ini dibuat dengan dasar coding java yang dikembangkan dalam software dari android.

4.3 Antar Muka Awal

Form ini merupakan tampilan awal ketika aplikasi ini di jalankan yang terdiri dari empat menu utama yaitu menu tulis pesan, menu kotak masuk menu kotak keluar dan menu keluar. Dapat dilihat pada Gambar 5.

Gambar 5. Form Menu

4.4 Form Menulis Pesan

Form ini berfungsi untuk membuat pesan terenkripsi sebelum pesan dikirim yang terdiri dari 4 EditText dan 3 Button, dapat dilihat pada Gambar 6.

Gambar 6. Form Menulis Pesan

4.5 Form Kotak Masuk

Menu ini berfungsi untuk menampilkan pesan terenkripsi untuk di dekripsi, dapat dilihat pada Gambar 7.

Gambar 7. Form Kotak Masuk

4.6 Proses Enkripsi

Uji coba sistem dibutuhkan untuk memeriksa apakah sistem yang dibua tsudah sesuai rancangannya. Tujuan uji coba sistem adalah untuk memastikan semua fitur berfungsi dengan baik sesuai yang diharapkan oleh pengguna. Hasil pengujian proses enkripsi dapat dilihat pada Gambar 8. Tulisan merah adalah hasil dari enkripsi pesan dengan kunci yang digunakan 'jainalinux'

Gambar8. Proses Enkripsi SMS

V. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dalam pembuatan aplikasi sms kriptografi menggunakan metode AES, penulis dapat menarik kesimpulan sebagai berikut :

8) Algoritma AES dapat diimplementasikan pada telepon seluler berbasis Android, sebagai sistem keamanan pesan.
9) Cara mengamankan pesan dengan menggunakan algoritma AES mampu meningkatkan keamanan pengirim dan penerima SMS dengan cara enkripsi dan dekripsi untuk smartphone android. Dan ini membantu pengguna yang ingin menjaga keamanan dalam berkomunikasi khususnya lewat SMS dari pihak-pihak yang tidak diinginkan.

5.2. Saran

Adapun wujud saran untuk lebih memaksimalkan aplikasi ini adalah:

1) Menambahkan beberapa fitur yang dapat mempermudah penggunaan aplikasi, seperti copy dan paste teks, dan fitur-fitur lain;
2) Tampilan aplikasi masih monoton sehingga masih perlu banyak tambahan.

DAFTAR PUSTAKA

[1] Aryus, Doni. 2006. Kriptografy Keamanan Data dan Komunikasi. Yogyakarta : Graha Ilmu
[2] Bruce Schneier. 1996. AppliedCryptograp by: Protocols, Algorithms, and Source Code in C. USA : John Wiley & Sons, Inc
[3] Hermawan. S, Stephanus. 2011. Mudah Membuat Aplikasi Android. Yogyakarta : CV Andi Offset
[4] https://id.wikipedia.org/wiki/Android_(28sistem _operasi), Android (sistem operasi), diakses pada, tanggal 16 April 2015
[5] https://id.wikipedia.org/wiki/Flowchart, diakses pada, tanggal 15 April 2015
[6] Kromodimoeijo, S. 2009. Teori dan Aplikasi Kriptografi, SPK IT CONSULTING
[7] Lesmana, I. 2010. Aplikasi Pembangkit Kunci Berbasis Modifikasi Bilangan Fibonacci Pada Sandi Vigenere. Jakarta : Universitas Pembangunan Nasional Veteran Jakarta
[8] Menezes, A, VanOorschot, P, Vanstone, S. 1997. Handbook of Applied Cryptography. CRC Press, Inc.
[9] Munir, Rinaldi. 2006. Kriptografi. Bandung : Informatika Bandung
[10] Safaat H, Nazruddin. (2012), "Android Pemrgraman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android", Bandung :Informatika.