IMPLEMENTASI ALGORITMA ENKRIPSI AES DAN VIGENERE CIPHER PADA APLIKASI SMS BERBASIS ANDROID

Rantika Dwi Amaliasari

Program Studi Teknik Informatika-S1, Fakultas Ilmu Komputer,
Universitas Dian Nuswantoro Semarang
URL :http://dinus.ac.id
111201106404@mhs.dinus.ac.id

ABSTRACT

Exchange messages via SMS (Short Message Service) is a service that is popular among mobile phone users in Indonesia. However, messages sent via SMS can not guarantee the integrity of its safety. Therefore we need a security system that is able to maintain the confidentiality of messages sent via SMS. Science of cryptography can be implemented in building security systems. The messages will be sent via SMS should be encrypted in advance using a security application. Vigenere simple algorithm combined with AES cipher can be used to secure the contents of SMS that are considered important and confidential. Corresponding methods in the development of this system is the Rapid Application Development (RAD). In the RAD method will be explained phases of software development, ranging from business modeling phase, the phase of data modeling, process modeling phase, the phase formation of the application, and the last phase is the testing and turnover. So they make SMS application program Encryption is used to secure the SMS so that only the sender and the recipient can read the message.

Keywords: SMS, Encryption, Cryptography, Cipher Vigenere, Advanced Encryption Standard (AES).

I. PENDAHULUAN

Perkembangan teknologi di bidang komunikasi semakin tahun semakin maju. Barbagai perangkat lunak untuk mengembangkan aplikasi ponselpun bermunculan, diantaranya yang cukup dikenal luas adalah android. Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman *Short Message Service* (SMS). SMS merupakan salah satu layanan yang populer dan praktis pada telepon bergerak *(mobile device)*.

SMS sendirinya memiliki berbagai kelemahan yaitu SMS dibangun dengan sistem dan program yang sama, dan SMS bisa melakukan *roaming* jaringan setempat hingga ke jaringan asing. Kelemahan dari SMS lainnya adalah isi SMS yang dikirim terbuka di sistim penyedia jasa dan pegawainya sehingga beresiko terhadap penyadapan dan modifikasi. Dengan adanya beberapa keterangan diatas maka

dibutuhkan sebuah sistem keamanan pada layanan SMS (terutama untuk *SMS Snooping*, *SMS Intercept* dan campur tangan operator). Agar isi pesan hanya bisa dibaca maknanya oleh pengirim dan penerima, isi pesan sebelum dikirim melalui SMS harus dienkripsi terlebih dahulu dengan algoritma kriptografi, misalnya AES dan Vigenere *Cipher*.

II. LANDASAN TEORI

1. Vigenere Cipher

Vigener cipher mungkin adalah contoh terbaik dari *cipher* alfabet-majemuk 'manual'. Algoritma ini dipublikasikan oleh diplomat Perancis, Blase de Vigenerepada abad 16. Algoritma enkripsi jenis ini sangat dikenal karena mudah dipahami dan diimplementasikan. Teknik untuk menghasilkan *ciphertext* bisa dilakukan menggunakan subtitusi angka maupun bujursangkar *vigenere*. Teknik subtitusi dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser.

Tabel 1. Vigenere Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Rumus enkripsi vigenere cipher :

$Ci \equiv (Pi + Ki) mod\ 26$

Atau

Ci = (Pi + Ki) – 26 kalau hasil penjumlahan *Pi* dan *Ki* lebih dari 26

Rumus dekripsi vigener cipher :

$Pi \equiv (Ci - Ki) mod\ 26$

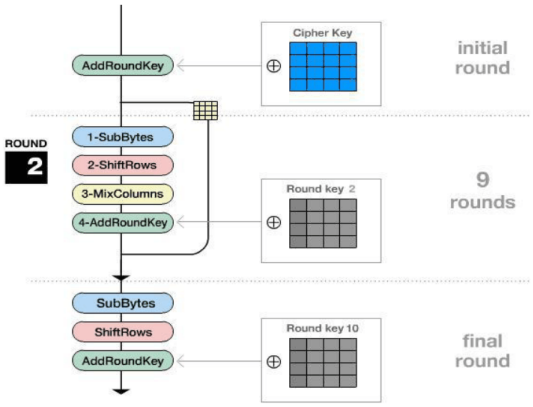
Atau

Pi = (Ci – Ki) + 26 kalau hasil pengurangan *Ci* dengan *Ki* minus.

2. Advanced Encryption Standard (AES)

DES (Data Encryption Standard) dianggap sudah tidak aman lagi karena dengan perangkat keras khusus kuncinya bisa ditemukan dalam beberapa hari, *National Institude of Standards and Technology (NIST),* sebagai agensi Departemen Perdagangan AS mengusulkan kepada Pemerintah Federal AS untuk sebuah standard kriptografi yang baru. Algortima *Rijndael* kemudian dikenal dengan *Advanced Encryption Standard* (AES). Setelah mengalami beberapa proses standarisasi oleh NIST, *Rijndael* kemudian diadopsi menjadi standard algoritma kriptografi secara resmi pada 22 mei 2002, pada tahun 2006, AES merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik.

Secara garis besar algoritma enkripsi Rijndael diperlihatkan pada gambar dibawah ini.



Gambar 1. Proses enkripsi AES

Garis besar Algoritma *Rijndael* yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut :

1. *AddRoundKey* : melakukan XOR antara state awal (*plaintext*) dengan

cipher key. Tahap ini disebut juga dengan *initial round*

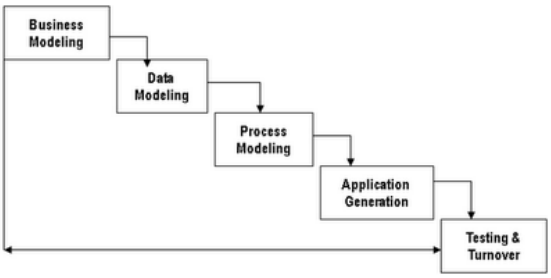
2. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah :
   a) *SubBytes :* subtitusi byte dengan menggunakan tabel subtitusi (S-box).
   b) *ShiftRows :* pergeseran baris-baris array state secara wrapping.
   c) *MixColumns* : mengacak data di masing-masing kolom array state.
   d) *AddRoundKey* : melakukan XOR antara state sekarang round key
3. *Final round* : proses untuk putaran terakhir.
   a) *SubBytes*
   b) *ShiftRows*
   c) *AddRoundKey*

III. METODE PENELITIAN

Metode Pengembangan Sistem

Agar mempermudah dalam pengembangan sistem, maka penulis membangun sebuah sistem yang akan membantu dalam menggambarkan proses penyelesaian masalah. Metode yang sesuai dalam pengembangan sistem ini adalah metode Rapid Aplication Development (RAD).

RAD adalah sebuah model proses perkembangan software sekuensial linier yang menekankan siklus perkembangan yang sangat pendek. Model ini merupakan sebuah adaptasi "kecepatan tinggi" dari model sekuensial linier dimana perkembangan cepat dicapai dengan menggunakan penekatan konstruksi berbasis komponen.

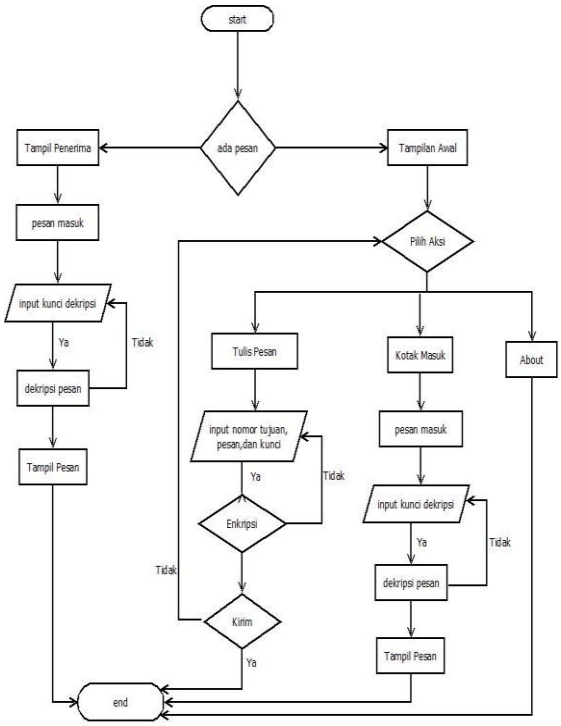


Gambar 2. fase-fase RAD

IV. RANCANGAN SISTEM DAN IMPLEMENTASI

1. Perancangan Alur Sistem Diagram

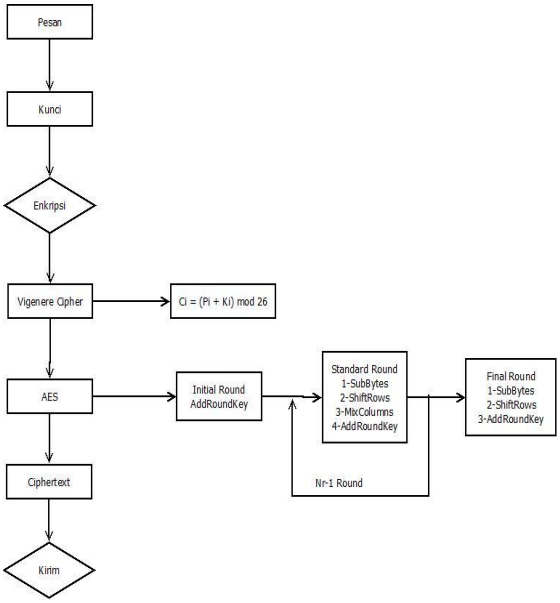
Berikut merupakan flowchart diagram alur sistem.



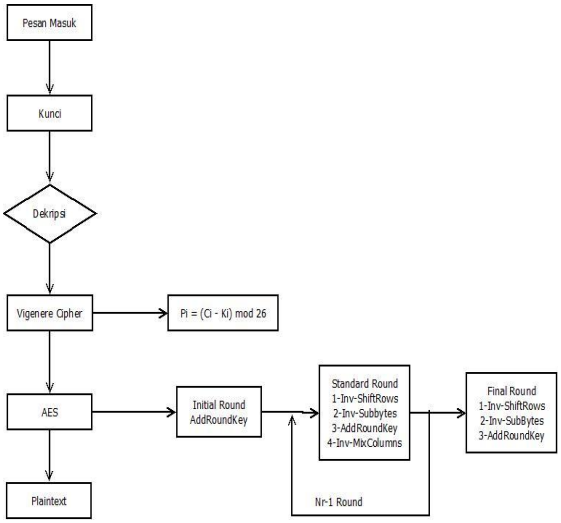
Gambar 3. Diagram Alur Sistem

2. Diagram Alur SMS Enkripsi/Dekripsi

Berikut diagram alur yang menjelaskan proses dari enkripsi dan dekripsi pesan.

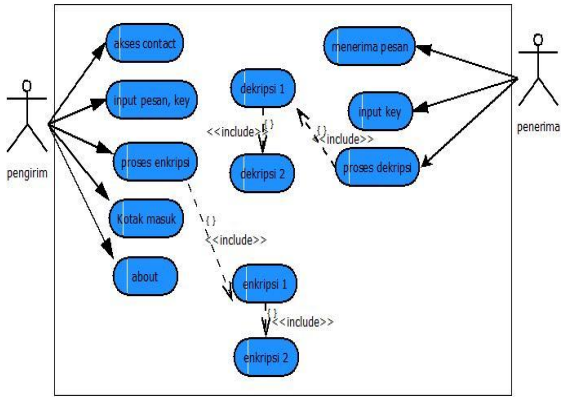


Gambar 4. Diagam alur sms enkripsi



Gambar 5. Diagram Alur SMS Dekripsi

3. Usecase Diagram



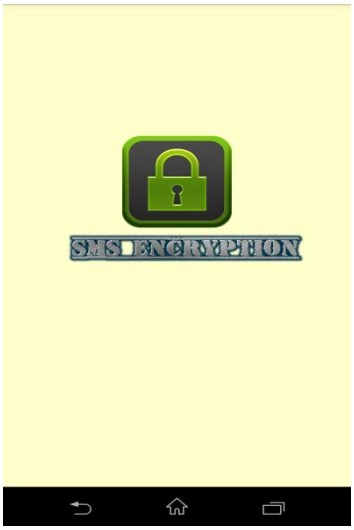
Gambar 6. Usecase diagram

Use case diagram SMS Encryption menceritakan tentang user yang menggunakan aplikasi ini secara optional bisa memilih untuk mengakses menu sesuai dengan yang diinginkan, fungsi utama dari aplikasi ini semuanya terletak pada halaman utama setelah dijalankan.

V. HASIL PENELITIAN DAN PEMBAHASAN

1. Analisa Percobaan

Saat user membuka aplikasi, akan muncul *Splashscreen* sekitar 5 detik. Kemudian pengguna akan masuk ke halaman utama.

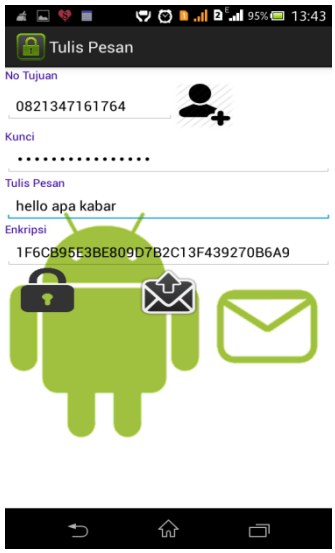


Gambar 6. Splash screen

Pada halaman menu ini terdapat 3 menu yaitu, menu tulis pesan, menu kotak masuk, dan menu about. Berikut ini merupakan tampilan menu utama pada aplikasi SMS Encryption.

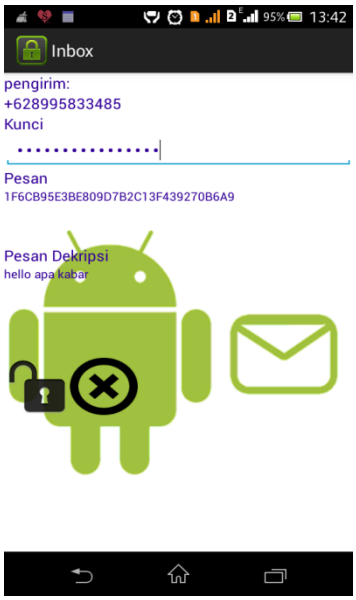
Gambar 7. Menu Utama

Pada proses ujicoba aplikasi ini, peneliti memasukkan nomor tujuan penerima, dengan kunci "dianuswantorosmg" dan *plaintext* (pesan) "hello apa kabar". Lalu dengan menekan button enkripsi dengan icon gembok akan menghasilkan pesan terenkripsi. Setelah itu menekan tombol kirim pesan, dan pengirim akan mendapatkan laporan pengiriman pesan.



Gambar 8. Proses Enkripsi pesan

Untuk proses dekripsi, jika ada pesan enkripsi masuk maka tampilan akan otomatis membuka form inbox yang berisi nomor pengirim, dan pesan yang terenkripsi. Lalu dengan menginputkan kunci yang sama saat mengenkripsi yaitu "dianuswantorosmg" maka pesan asli akan dapat terbaca "hello apa kabar". Setelah itu dengan menekan button keluar untuk mengakhiri aplikasi, dan aplikasi yang sudah terdekripsi akan otomatis terhapus.



Gambar 9. Proses Dekripsi pesan

2. Pengujian Blacbox Testing

Berdasarkan hasil pengujian, dapat diperoleh kesimpulan bahwa performansi program cukup baik. Semua rancangan program telah tersusun dalam menu dengan tepat dan setiap kontrol yang terdapat tipa-tiap menu juga dapat diakses secara tepat.

Tabel 2. Blackbox Testing

Faktor Pengujian	Status Output
Menu tulis pesan	Baik
Menu kotak masuk	Baik
Menu about	Baik
Button enkripsi	Baik
Button kirim	Baik
Button dekripsi	Baik

3. Kuisoner

Pengujian selanjutnya dilakukan untuk mengetahui respon dari user terkait dengan program yang telah penulis buat sebelumnya dan telah diujicobakan. User yang menjadi responden adalah mahasiswa Universitas Dian Nuswantoro Semarang. Kepada masing-masing responden, peneliti membagikan kuisoner yang berbentuk isian pilihan penilaian terhadap software aplikasi SMS Encryption yang sebelumnya telah diujicobakan.

Tabel 3. Kuisoner

No	Pertanyaan	Nilai				
		1	2	3	4	5
A	Kemampuan Software					
1	Apakah pesan tersembunyi dengan baik?					
2	Bagaimana kinerja program aplikasi?					
3	Apakah program dapat mengirimkan pesan?					
4	Apakah aplikasi dapat mengembalikan pesan seperti semula?					
B	Interaksi Manusia dan Komputer					
1	Apakah pengguna dapat menggunakannya dengan baik?					
2	Bagaimana bentuk design aplikasi?					
3	Apakah program berjalan dengan lancar?					
4	Bagaimana tampilan menu aplikasi?					

VI. KESIMPULAN

Dari penelitian yang dilakukan dapat diambil kesimpulan yaitu :

1. Aplikasi dapat mengirimkan pesan terenkripsi dan dapat melakukan dekripsi kembali apabila kunci yang dimasukkan sudah sesuai.
2. Dua belah pihak pengguna harus sama-sama menginstal aplikasi ini untuk bisa bertukar pesan rahasia.
3. Penelitian ini tidak lebih baik dibanding dengan penelitian yang dilakukan oleh Imam Prayogo[13], karena pertukaran kunci antara pengirim dan penerima masih dilakukan secara lisan, sehingga pihak lain bisa mengetahui kunci rahasia tersebut.
4. Penelitian ini masih kurang tepat, karena sudah banyak aplikasi enkripsi pesan yang berkembang pada perangkat mobile terdahulu.

Daftar Pustaka

[1] Munir, Rinaldi, *Kriptografi*. Bandung: Informatika, 2006.

[2] Andi Kurniawan Dwi P, "Penerapan Algoritma Vigenere Cipher pada Aplikasi SMS Android," Bandung, 2011/2012.

[3] Noni Endriani, "Implementasi Algoritma AES pada Aplikasi SMS Berbasis Android," Yogyakarta, 2014.

[4] Andi Pahri. (2012, Oct.) Academia. [Online]. www.academia.edu/4844015/Metode_pengembangan_perangkat_lunak

[5] Nazruddin Safaath, *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC berbasis Android*. Bandung: Informatika, 2012.

[6] Zaenal Muttaqin, "Pembuatan Aplikasi Enkripsi Menggunakan Metode AES dan RSA," Universitas Islam Negeri Syarif Hidayatullah, Jakarta, skripsi 2010.

[7] Mukhlisulfatih L, Rochmad MTJ Arif Dwinanto, "Penerapan Algoritma AES 128 dan Vigenere Cipher pada Aplikasi Enkripsi Pesan Singkat Android," Universitas Negeri Gorontalo, Gorontalo, Penelitian 2014.

[8] Anonimous. (2014, Oct.) wikipedia. [Online]. http://id.wikipedia.org/wiki/Layanan_pesan_singkat

[9] Anonimous. (2014, Nov.) Daftar versi Andoid. [Online]. http://www.id.m.wikipedia.org/wiki/Daftar_versi_Android

[10] Anonimous. (2014, Nov.) wikipedia

Indonesia. [Online]. http://www.id.m.wikipedia.org/wiki/Advanced_Encryption_Standard

[11] Muhammad Humam, "Peningkatan Keamanan Algoritma DES Pada Aplikasi Enkripsi SMS Android Menggunakan Algoritma AES 256 Bit," Universitas Dian Nuswantoro, Semarang, Skripsi 2014.

[12] Adetya Krisna Prastyo, "Pengamanan Data Dengan Metode Advanced Encryption Standard dan Metode Least Significant Bit," Universitas Dian Nuswantoro, Semarang, Skripsi 2014.

[13] Imam Prayogo Pujiono, "Implementasi Algoritma AES dan Modifikasi Vigenere untuk Pengaman Pesan SMS dengan Nomor Pengirim dan Penerima Sebagai Kunci Tambahan," Udinus, Semarang, 2015.