KEAMANAN KOMUNIKASI DATA SMS PADA ANDROID DENGAN MENGGUNAKAN APLIKASI KRIPTOGRAPI ADVANCE ENCRYPTION STANDARD (AES)

Erwin Gunadhi[1], Harry Abdurachman[2]

Jurnal Algoritma
Sekolah Tinggi Teknologi Garut
Jl. Mayor Syamsu No. 1 Jayaraga Garut 44151 Indonesia
Email : jurnal@sttgarut.ac.id

[1]erwin.gunadhi@sttgarut.ac.id
[2] 1106052@sttgarut.ac.id

Abstrak – *Penggunaan ponsel pintar (smartphone) di masyarakat saat ini sangat luas. Android menjadi yang paling diunggulkan oleh para pengguna dan juga produsen smartphone karena fiturnya yang sangat menarik. Namun demikian, meskipun teknologi dari smartphone ini memiliki banyak fitur, pengguna masih memiliki perhatian khusus terhadap SMS (Short Message Service). Sayangnya, fitur SMS ini memiliki keterbatasan terutama dalam keamanan pertukaran informasi yang bersifat rahasia, sehingga dibutuhkan sistem yang dapat memberikan pengamanan terhadap pertukaran informasi pada SMS berbasis android. Oleh karena itu, diperlukan metode untuk mengamankannya, salah satunya dengan menggunakan metode kriptografi. Metode yang digunakan pada penelitian tugas akhir ini adalah Advance Encryption Standard (AES), Hasil yang diperoleh pada penelitian tugas akhir ini adalah sistem keamanan data SMS berbasis android.*

Kata Kunci *– Short Message Service,* keamanan komunikasi data, kriptograpi Advance Encryption Standard (AES), Android.

I. PENDAHULUAN

Beberapa tahun terakhir ini terjadi perkembangan yang pesat pada teknologi, salah satunya adalah telepon selular (ponsel). Mulai dari ponsel yang hanya bisa digunakan untuk bicara dan sms hingga "ponsel cerdas" (*smart phone*) yang memiliki berbagai fungsi seperti *multimedia*, *multiplayer games*, transfer data, video *streaming* dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponselpun bermunculan, diantaranya yang cukup dikenal luas adalah Java 2 *Micro Edition* (J2ME). Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman data berupa pesan singkat melalui *Short Message Service* (SMS). Dengan fasilitas SMS kita bisa bertukar informasi, mengobrol dan melakukan percakapan jarak jauh berupa teks yang terjadi antara dua belah pihak tanpa ada yang mengetahui apa yang di informasikan dan diperbincangkan.

Di sisi lain adanya aplikasi sadap SMS, mungkin ini terdengar mengerikan bagi orang awam. Sadap atau menyadap biasanya indentik dengan hal-hal yang berarti negatif. Sadap juga bisa diartikan sebagai tindakan untuk memata-matai, mengawasi bahkan kepada tindakan yang merugikan.

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama informasi sensitif yang hanya boleh diketahui oleh pihak yang berhak saja. Informasi yang merupakan hasil pengolahan dari data, mempunyai nilai yang berbeda bagi setiap orang. Seringkali sebuah informasi menjadi sangat berharga dan tidak semua orang diperkenankan untuk mengetahuinya, namun selalu saja ada pihak yang berusaha untuk mengetahui informasi dengan cara-cara yang tidak semestinya bahkan bermaksud untuk merusaknya.

Kesenjangan yang terjadi pada waktu sekarang ini adalah timbulnya suatu pertanyaan bagaimana cara mengamankan informasi rahasia seseorang yang dikirimkan melalui fasilitas SMS? Karena seperti diketahui tidak ada fitur dalam sms yang bisa digunakan untuk mengamankan pesan atau

informasi yang bersifat rahasia, sehingga terjadi kebocoran informasi yang disalah gunakan dan merugikan berbagai pihak.

Beberapa penelitian tentang aplikasi enkripsi sms pada android dengan metode advance encryption standard telah dilakukan diantaranya "Aplikasi sms pada telpon seluler berbasis J2ME dengan metode vighenere Cipher" [1]. Penulis membedakan metode dan algoritma dalam penelitian ini dengan penelitian sebelumnya, sehingga isi dan perancangan sistem yang akan di lakukan berbeda dengan penelitian yang sudah ada.

Berdasarkan pada latar belakang diatas, penulis bermaksud meneliti dan mengimplementasikandalam berupa aplikasi melalui sebuah penelitian dengan judul

"KEAMANAN KOMUNIKASI DATA SMS PADA ANDROID DENGAN MENGGUNAKAN APLIKASI KRIPTOGRAPI ADVANCE ENCRYPTION STANDARD (AES)"

II. LANDASAN TEORI

A. Teknologi telekomunikasi

Teknologi informasi dan komunikasi mempermudah kehidupan manusia. Jika menggunakan alat teknologi informasi dan komunikasi, dua benua akan terasa tidak berjarak. Kehadiran komputer, internet, telepon seluler, dan berbagai alat teknologi informasi dan komunikasi membuat arus informasi semakin lancar. Teknologi informasi dan komunikasi memuat semua teknologi yang berhubungan dengan penanganan informasi. Penanganan ini meliputi pengambilan, pengumpulan, pengolahan, penyimpanan, penyebaran, dan penyajian informasi. Jadi, teknologi telekomunikasi adalah teknologi yang berhubungan dengan pengambilan, pengumpulan, pengolahan, penyimpanan, penyebaran, dan penyajian informasi [2].

B. Ancaman Keamanan Dalam Komunikasi Data

Tingginya lalu lintas pertukaran informasi setiap detik di internet, baik itu komunikasi kabel maupun tanpa kabel (*wireless*), mendorong terjadinya pencurian informasi oleh pihak-pihak yang tidak bertanggung jawab. Ancaman keamanan yang terjadi terhadap informasi adalah:

1. *Interruption*

Merupakan suatu ancaman terhadap availabilitas, informasi, data yang ada dalam sistem computer di rusak, dihapus, sehingga jika data atau informasi tersebut di butuhkan maka menjadi tidak ada lagi.

2. *Interception*

Merupakan ancaman terhadap kerahasiaan (*secrecy*), informasi yang ada di sadap atau orang yang tidak berhak mendapat akses ke komputer di mana informasi tersebut di simpan.

3. *Modification*

Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan diubah sesuai keinginan orang tersebut.

4. *Fabrication*

Merupakan ancaman terhadap integritas, yaitu orang yang tidak berhak yang meniru atau memalsukan informasi yang ada sehingga orang yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi tersebut [2].

C. Pengertian Keamanan system

Masalah keamanan merupakan salah satu aspek penting dari sebuah system informasi. Sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan [3].

Sistem adalah Sekumpulan hal atau kegiatan atau elemen atau subsistem yang salingbekerja sama atau yang di hubungkan dengan cara – cara tertentu sehingga membentuk satu kesatuan untuk melaksanakan suatu fungsi guna mencapai suatu tujuan [2]

D. Pengertian Kemanan Data

Tingkatan pada keamanan data adalah :

1.Fisikal : lokasi-lokasi dimana terdapat sistem komputer haruslah aman secara fisik terhadap serangan perusak.
2.Manusia : wewenang pemakai harus dilakukan dengan berhati-hati untuk mengurangi kemungkinan adanya manipulasi oleh pemakai yang berwenang
3.Sistem Operasi : Kelemahan pada SO ini memungkinkan pengaksesan data oleh pihak tak berwenang, karena hampir seluruh jaringan sistem basis data menggunakan akses jarak jauh.
4.Sistem Basis Data : Pengaturan hak pemakai yang baik [3].

E. Kriptograpi

Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata kriptografi dibagi menjadi dua, yaitu kripto dan graphia. Kripto berarti *secret* (rahasia) dab graphia berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat menuju tempat yang lain. Dalam perkembangannya, kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan dengan sidik jari digital (*fingerprint*) [3]

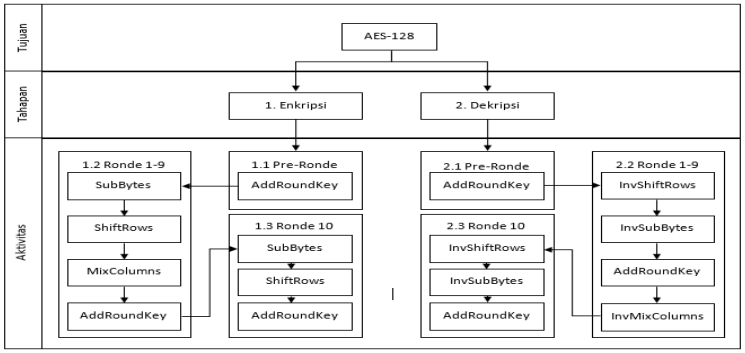
F. AES

AES (*Advanced Encryption Standard*) adalah cipher blok yang akan menggantikan DES. Pada bulan Januari 1997 inisiatif AES diumumkan dan pada bulan September 1997 publik diundang untuk mengajukan proposal block cipher yang cocok sebagai kandidat untuk AES. Pada tahun 1999 NIST mengumumkan lima kandidat finalis yaitu MARS, RC6, Rijndael, Serpent, dan Twofish. Algoritma AES dipilih pada bulan Oktober 2001 dan standarnya diperkenalkan pada bulan November 2002. AES mendukung ukuran kunci 128 bit, 192 bit, dan 256 bit, berbeda dengan kunci 56-bit yang ditawarkan DES. Algoritma AES dihasilkan dari proses bertahun-tahun yang dipimpin NIST dengan bimbingan dan review dari komunitas internasional pakar kriptografi. Algoritma Rijndael yang dikembangkan oleh Joan Daemen dan Vincent Rijmen dipilih sebagai standar enkripsi [4].

III. KERANGKA KERJA KOSEPTUAL

Aktivitas dimulai dari penentuan latar belakang yang akan menjelaskan secara garis besar mengenai penelitian ini dimulai dari merumuskan masalah. Kemudian rumusan masalah tersebut dijadikan sebagai acuan untuk membuat sebuah tujuan penelitian. Setelah tujuan ditentukan, tahap selanjutnya adalah mencari dan merumuskan studi literatur dengan melakukan penelaahan terhadap buku-buku yang terkait dengan penelitian ini untuk dijadikan sebagai acuan penelitian agar mendukung terhadap tujuan penelitian yang dilihat dari sisi ilmiah. Kemudian disusun *Work Breakdown Structure* (WBS). Dari WBS yang dirancang dengan menggunakan literatur dihasilkan rancangan *activity sequence* dan *detail activity* penelitian yang diterapkan kedalam tahapan penelitian. Setelah WBS dibuat kemudian dilakukan pembahasan dari tahapan-tahapan penelitian mulai dari semua aktivitas yang akan menghasilkan suatu kesimpulan dari penelitian yang telah dilakukan.

Berikut ini adalah skema kerangka kerja konseptual secara mendetail:



Gambar *Activity Sequence*

IV. HASIL DAN PEMBAHASAN

A. Ancaman Keamanan Data

Komunikasi data SMS tidak luput dari ancaman – ancaman baik berupa kesalahan ataupun serangan serangan orang ketiga yang bisa menghambat lajunya data asli yang bersifat rahasia. Ancaman – ancaman tersebut adalah sebgai berikut :

1. *Interruption*

Pengiriman sms yang tidak sampai sering terjadi pada komunikasi data sms di karenakan sinyal operator yang jelek dan mengatur jangka waktu sms 24 jam, sehingga apa yang saya kirimkan kepada teman saya tidak sampai tepat waktu. Maka dari itu *interruption* bukan salasatu bentuk kehandalan komunikasi data lewat sms.

2. *Interception*

Penyadapan yang sering terjadi pada komunikasi data sms yaitu menggunakan software sms *forwarder*, sehingga apa yang saya komunikasikan dengan temen saya bisa di sadap orang lain. Maka *interception* adalah salasatu bentuk kejahatan komunikasi data lewat sms.

3. *Modification*

Keaslian data sms yang di rubah atau di ganti oleh orang lain, sehingga pesan yang dikirimkan tidak asli lagi karena sudah di ganti oleh orang lain. Hal ini jarang terjadi pada komunikasi data lewat sms sehingga *modification* bukan ancaman yang terjadi pada komunikasi data sms.

4. *Fabrication*

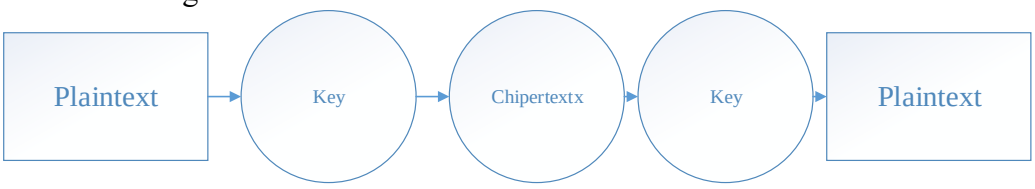
Pemalsuan yang sering terjadi pada komunikasi data sms yaitu orang lain yang mengatasnamakan saya mengirimkan pesan kepada teman saya, sehingga teman saya menyangka bahwa pesan tersebut berasal dari saya. Maka *fabrication* adalah salasatu bentuk kejahatan komunikasi data lewat sms.

Penulis menjabarkan dari ke empat jenis kejahatan yang mungkin terjadi pada komunikasi data lewat sms adalah *interception* dan *fabrication*

B. Kriptograpi

Kerahasiaan data SMS rentan bocor akibat pihak ketiga yang berhasil mendapatkan akses informasi dari dalam sistem komunikasi, penanggulangan masalah ancaman tersebut harus di pecahkan dengan penguncian data enkripsi yang akan di deskripsi oleh penerima.

Berdasarkan pembahasan di atas maka penulis membuat sebuah aplikasi/kriptograpi menggunakan AES untuk mengamankan data lewat sms :

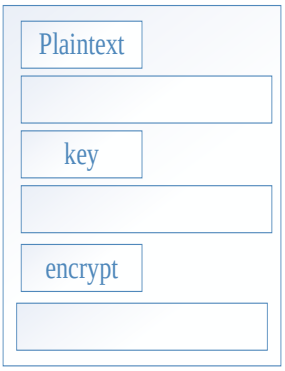


Gambar Penguncian data enkripsi yang akan di Deskripsi

Pesan “Harry” di dalam plainteks merupakan data yang akan dikirim. Terdapat *key* atau kunci yang hanya bisa di buka oleh si penerima. Kata kunci itu adalah “08989355352”Enkripsi dari plainteks “Harry” adalah “06731C1C6F4A0F07300F6B0509791C1B” yang nantinya akan di deskripsikan oleh si penerima. Setelah si penerima membuka dengan kunci “08989355352” untuk mendeskripsikan pesan yang terenkripsi dengan kode enkripsi “06731C1C6F4A0F07300F6B0509791C1B” maka deskripsi dari kata tersebut adalah “Harry”.

Di dalam gambar terdapat *key* atau kunci yang di rahasiakan dan hanya si penerima yang bisa mendeskripsikan data yang di kirim berupa enkripsi dengan membuka kunci yang ada pada gambar, sehingga pihak ketiga tidak akan bisa mengakses kerahasiaan data tersebut.

Berikut adalah rancangan pengiriman pesan, tulis pesan (Plaintext) masukan kunci (key) pesan yang dikirim (enkripsi).



Gambar Tampilan interface pengirim

Berikut adalah rancangan penerimaan pesan. Pesan masuk (chipertext) masukan kunci (key) pesan asli yang diterima (deskripsi).

Gambar Tampilan interface penerima

V. KESIMPULAN

Berdasarkan perancangan sistem keamanan komunikasi data SMS dapat diambil kesimpulan, yaitu sistem keamanan ini dapat digunakan untuk mengamankan komunikasi data sms dari ancaman-ancaman yang tidak berhak.

DAFTAR PUSTAKA

[1] B. K. Nugroho, "Aplikasi Enkripsi SMS pada Telepon Selular berbasis J2ME dengan Metode Vigenere Chiper," Diss. FACULTY OF MATHEMATICS AND NATURAL SCIENCES, 2010.

[2] A. Dony and R. K. Andri, Komunikasi Data, Yogyakarta: Andi, 2008.

[3] R. Budi, Keamanan Sistem Informasi Berbasis Internet, Jakarta, 2005.

[4] Admin, "Sistem Keamanan Data," 2009. [Online]. Available: http://www.academia.edu/7612178/SISTEM_KEAMANAN_DATA. [Accessed 26 July 2015].