SISTEM KEAMANAN *SHORT MESSAGE SERVICE (SMS)* BERBASIS ANDROID MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES)

Sugiyanto[1], Rinci Kembang Hapsari[2]
Jurusan Teknik Informatika Institut Teknologi Adhi Tama Surabaya
Jl. Arief Rachman Hakim 100, Surabaya
Email : [1]sugianto@itats.ac.id, [2]rincikembang@itats.ac.id

ABSTRACT
-

ABSTRAK

Handphone pintar mempunyai banyak fitur, namun fitur lama seperti layanan pesan singkat atau yang lebih dikenal dengan SMS (Short Message Service) masih banyak yang menggunakan. Agar isi SMS hanya dapat dibaca informasinya oleh pengirim dan penerima, maka isi pesan sebelum dikirim harus dienkripsi terlebih dahulu. Dengan melakukan enkripsi terhadap isi SMS maka tingkat keamanan informasi dari sebuah pesan dapat ditingkatkan. Pada penelitian ini dibuat sistem keamanan SMS yang dapat menjaga keamanan isi pesan untuk bisa menutupi celah keamanan pesan. Isi pesan tersebut sebelum dikirim melalui layanan SMS terlebih dahulu harus dienkripsi dengan algoritma kriptografi Advanced Encrytion Standard (AES). Sistem keamanan Short Message Service (SMS) berbasis android menggunakan algoritma Advanced Encryption Standard (AES) dapat mengirim SMS, dan memiliki fungsi merubah isi SMS menjadi chipertext agar isi informasi SMS tidak deketahui oleh orang lain.

Kata kunci : SMS, enkripsi, Android, Advanced Encryption Standard.

PENDAHULUAN

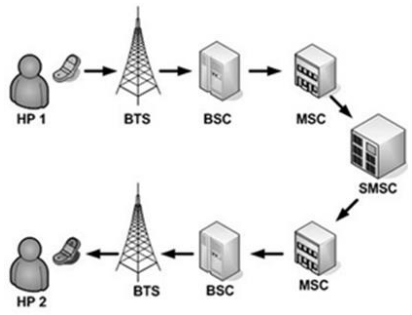
Perkembangan teknologi telepon selular *(handphone)* untuk beberapa tahun ini sangat pesat. Sekarang banyak handphone pintar yang mempunyai sistem operasi Android. Meskipun handphone pintar mempunyai banyak fitur, namun fitur lama seperti layanan pesan singkat atau yang lebih dikenal dengan SMS *(Short Message Service)* masih banyak yang menggunakan [1]. Dengan fasilitas SMS yang ada, mulai timbul pertanyaan apakah keamanan pada SMS bisa dijamin. Agar isi SMS hanya dapat dibaca informasinya oleh pengirim dan penerima, maka isi pesan sebelum dikirim harus dienkripsi terlebih dahulu. Enkripsi merupakan proses merubah plaintext (pesan yang dapat dibaca) dirubah menjadi chipertext (pesan yang tidak dapat dibaca). Kebalikan dari enkripsi adalah deskripsi. Dengan melakukan enkripsi terhadap isi SMS maka tingkat keamanan informasi dari sebuah pesan dapat ditingkatkan.

Model enkripsi yang sering digunakan adalah MD5 (Message-Digest algorithm 5). MD5 menerima sembarang ukuran masukan dan mengkonversi masukan tersebut dengan algoritma hash menjadi message digest yang berukuran 128 bit atau 32 digit karakter heksadesimal. MD5 juga mempunyai sifat *'collision free'* yaitu tidak mungkin 2 pesan yang berbeda memiliki enkripsi MD5 yang sama. MD5 pada umumnya digunakan untuk keperluan integritas dan otentikasi pesan [2]. Enkripsi lainnya adalah SHA1 (Secure Hash Algorithm) yang merupakan sebuah fungsi hash satu arah yang diciptakan oleh NIST dan digunakan dengan DSS (Digital Signature Standart). SHA1 menerima sembarang ukuran masukan dan menghasilkan message digest yang mempunyai panjang 160 bit, lebih panjang dari message digest yang dihasilkan oleh MD5 [3]. Pada penelitian ini dibuat sistem keamanan SMS yang dapat menjaga keamanan isi pesan untuk bisa menutupi celah keamanan pesan. Isi pesan tersebut sebelum dikirim melalui layanan SMS terlebih dahulu harus dienkripsi dengan algoritma kriptografi *Advanced Encrytion Standard (AES).*

TINJAUAN PUSTAKA

Short Message Service (SMS)

Short Message Service (SMS) adalah sebuah layanan yang mempunyai fasilitas pertukaran pesan singkat antara orang satu dengan yang lainnya. SMS diaplikasikan pada jaringan komunikasi tanpa kabel yang memungkinkan dalakukannya pengiriman pesan dalam bentuk alphanumeric antar terminal pelanggan (ponsel) atau antara terminal pelanggan dengan sistem eksternal seperti e-mail, pagging, voice mail dan sebagainya [4]. Di dalam sebuah jaringan GSM pada umumnya terdapat beberapa perangkat diantaranya BTS, BSC, MSC/VLR, HLR dan SMSC. Base Station Controler (BTS) berfungsi sebagai transceiver yang melakukan komunikasi dengan semua *handphone* yang aktif dan dalam cakupan wilayahnya (cell). Base Station Controller (BSC) mengatur beberapa BTS yang menjadi cakupannya, yang berfungsi konfigurasi cell site, handover, tuning power, sumber daya radio dan frekuensi pada BTS. Mobile Switching Center (MSC) berfungsi melakukan switching dan melakukan pengaturan terhadap call setup, panggilan, routing dan release. MSC juga berfungsi sebagai gateway ke jaringan lainnya dan melakukan fungsi billing (terhubung pada *billing system*). Dari MSC, sebuah jaringan selular dapat berkomunikasi dengan jaringan lainnya. Short Message Service Center (SMSC) berfungsi sebagai penyampai pesan SMS antara Mobile Station (MS) dengan *handphone*, dan juga berfungsi sebagai store-and-forwarding SMS jika nomor penerima tidak aktif. Di dalam sebuah jaringan terdapat operator yang mempunyai lebih dari satu sebuah perangkat SMSC, disesuaikan dengan luasnya trafik jaringan tersebut. Alur SMS dapat dilihat pada gambar 1.



Gambar 1. Alur SMS

Keterangan:
BTS : Base Transceiver Station
BSC : Base Station Controller
MSC : Mobile Switching Center
SMSC : Short Message Service Center

Serangan pada *Short Message Service (SMS)*

Jika pengguna melakukan *Short Message Service (SMS)* maka rentan terhadap beberapa serangan diantaranya :

1. ***Man-in-middle Attack***. Sebuah serangan dimana penyerang akan berada pada tengah-tengah komunikasi antara pengirim dan penerima. Seluruh pesan yang terkirim antara pengirim dan penerima harus melalui penyerang terlebih dahulu. Penyerang dengan bebas melakukan pencegatan, penyadapan, pengubahan, bahkan dapat memalsukan komunikasi antara pengirim dan penerima.
2. ***Replay Attack***. Penyerang berpura-pura sebagai user yang autentik atau user yang asli.
3. ***Message Disclosure***. Pesan yang dikirim tidak dienkripsi terlebih dahulu maka pesan yang terkirim disimpan pada SMSC sebelum dikirimkan pada penerima akan disimpan dengan teks biasa, sehingga operator pada SMSC akan dapat dengan mudah melihat isi dari pesan.
4. ***Spamming***. Penyerang mengirim sebuah junk message yang dikirim sebagai pesan text melalui Short Message Service (SMS). Penyerang mengirimkan pesan ini dalam volume atau jumlah yang besar sehingga Handphone korban tidak dapat digunakan.

5. ***Denial of Service (DOS) Attack.*** Sebuah serangan dimana penyerang mengirim pesan berulang-ulang pada target serang, yang bertujuan agar handphone korban tidak bisa digunakan atau error.
6. ***SMS Phone Crasher***. Sebuah serangan dimana penyerang mengirim pesan yang cacat pada korban, sehingga handphone korban akan terinfeksi dan tidak bisa dioperasikan.

Kriptografi

Pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah kriptografi tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi [5]. Di dalam kriptografi, akan sering ditemukan berbagai istilah. Adapun istilah yang sering digunakan yaitu:

a. Pesan adalah sebuah data atau informasi yang dapat dibaca dan mudah dimengerti maknanya oleh seseorang yang membutuhkannya.
b. Ciphertext adalah suatu bentuk pesan yang acak dan tidak bisa dimengerti pesannya. Pesan dibuat acak agar pesan tersebut tidak bisa dimengerti atau dibaca informasi yang ada didalamnya.
c. Pengirim dan penerima. Suatu pekerjaan komunikasi data, pasti akan melibatkan pertukaran dua objek, yaitu seorang pengirim dan seorang yang menerima. Pengirim adalah sebuah objek yang mengirimkan sebuah pesan pada penerima, sedangkan penerima adalah sebuah objek yang menerima pesan dari pengirim.
d. Enkripsi dan Deskripsi. Suatu proses yang merubah plaintext (kalimat yang jelas maknanya) menjadi chipertext (kalimat yang tidak jelas maknanya) disebut dengan enkripsi (*encryption*). Deskripsi (*decryption*) adalah suatu proses merubah chipertext menjadi plaintext kembali.

2.4 Advanced Encryption Standard (AES)

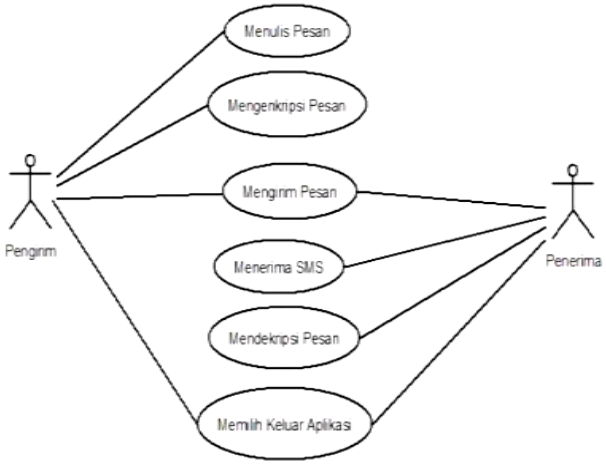
Algoritma AES adalah algoritma yang menggunakan proses substitusi, permutasi, dan sejumlah putaran (cipher berulang). Setiap putaran kunci (round key) menggunakan kunci yang berbeda [6]. Algoritma AES beroperasi dalam orientasi byte, sedangkan DES beroperasi dalam orientasi bit. Selain itu, AES tidak menggunakan jaringan Feistel seperti DES dan GOST [7]. Algoritma AES:Rijndael mempunyai tiga komponen :

1. *Plaintext* : data masukan yang berbentuk *array* yang berukuran 16 *byte*.
2. *Ciphertext* : hasil dari enkripsi yang berbentuk *array* berukuran 16 *byte*.
3. *Key* : kunci (*cipher key*) yang berbentuk *array* yang berukuran 16*byte*.

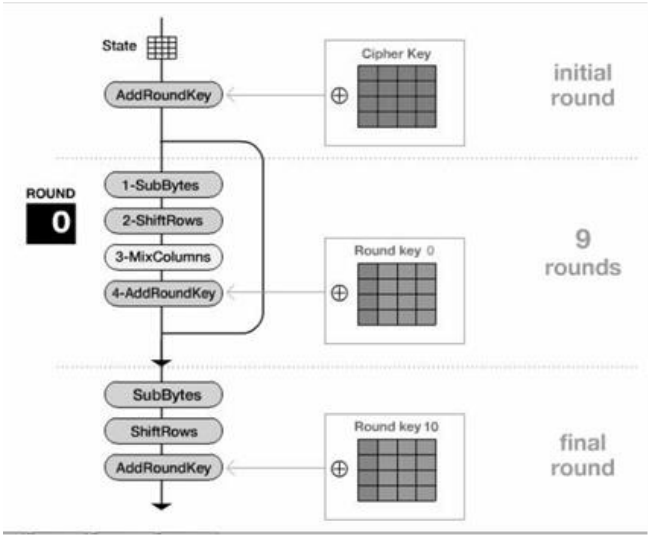
Dengan 16 *byte*, maka baik blok data dan kunci yang berukuran 128-bit dapat disimpan di dalam ketiga *arraystate* tersebut. Selama proses kalkulasi dari plainteks menjadi cipherteks, data disimpan dahulu didalam *array of bytes* dua dimensi, state, yang berukuran N_{ROWS} *x* N_{COLS}. Untuk blok data 128 bit state tersebut berbentuk seperti matriks ordo 4 x 4 [8].

METODE PENELITIAN

Sistem keamanan pesan pada layanan SMS dibuat ini menggunakan algoritma kriptografi Advanced Encryption Standard (AES). Untuk proses enkripsi maupun dekripsi pesan dari algoritma Advanced Encryption Standard (AES) dapat dilihat pada Use Case Diagram pada gambar 2. Use Case Diagram digunakan untuk menggambarkan skenario yang terjadi dalam aplikasi. Diagram ini memiliki dua aktor yaitu pengirim dan penerima. Pada gambar 2 menggambarkan pengirim dapat menulis pesan, mengenkripsi pesan, mengirim pesan, serta memilih keluar aplikasi. Untuk penerima dapat mengirim pesan, menerima SMS, mendekripsi pesan, serta memilih keluar aplikasi. Proses enkripsi dari algoritma AES dapat dilihat pada gambar 3.



Gambar 2. Use Case Diagram



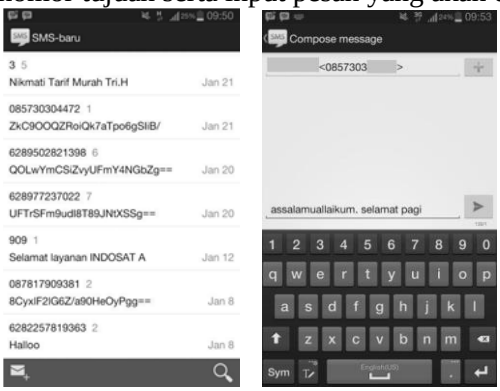
Gambar 3. Diagram Proses Enkripsi

Pada proses AddRoundKey, plainteks akan digabungkan dengan kunci (cipherkey) dengan menggunakan operasi XOR untuk setiap byte dari plainteks dengan byte pada kunci (cipherkey). Setiap hexadecimal yang ada di dalam state diubah dalam bentuk biner untuk proses perhitungan XOR. Hasil dari XOR tersebut dimasukkan kedalam array state sehingga dihasilkan array state. Proses SubBytes adalah proses substitusi tidak linear dengan cara mengganti setiap byte yang ada dalam arraystate dengan byte pada tabel S-box. Proses ShiftRows beroperasi pada tiap baris pada arraystate. Proses ini bekerja dengan cara menggeser atau memutar bytes-bytes pada baris terakhir yaitu pada baris 1, 2, dan 3, dengan jumlah pergeseran yang berbeda-beda.

Pada proses *MixColumns* akan dilakukan pengacakan *array state*, yaitu dengan cara melakukan perkalian matriks antara tiap kolom yang merupakan transformasi dari perkalian polinom dengan polinom 4 suku pada GF(2^8). Dalam proses perkalian ini untuk menjadikan hasil perkalian menjadi bentuk biner 8 bit, maka bilangan tersebut diubah menjadi 1 bit dan dilakukan pergeseran ke kiri sebanyak 1 bit pada bilangan hexadesimal yang telah diubah kedalam biner. Proses *Key Schedule* terbentuk dari pengambilan kunci cipher (*cipherkey*) dan melakukan rutin dari ekspansi kunci (*key expansion*).

HASIL DAN PEMBAHASAN

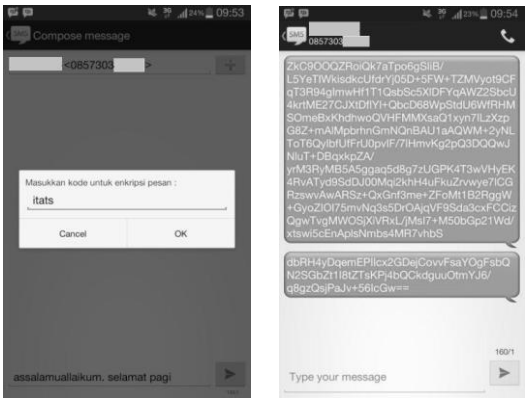
Pada gambar 4 (a) menampilkan list pesan masuk dari pengirim dan terdapat juga button untuk menulis pesan baru, serta ada button search untuk mencari pesan yang ada dalam list. Gambar 4(b) menampilkan proses input nomor tujuan serta input pesan yang akan dikirim oleh user.



(a) (b)

Gambar 4. (a)Tampilan Inbox pesan; (b) Tampilan menulis pesan baru

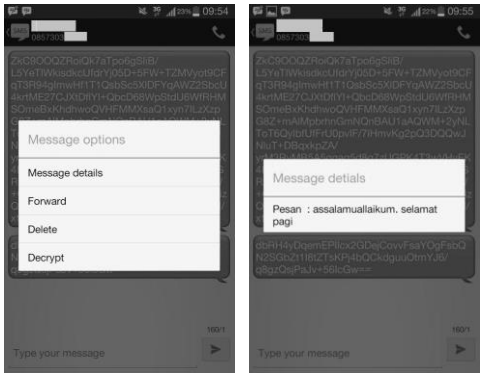
Pada gambar 5 (a) Menampilkan proses input kunci atau kode untuk enkripsi pesan yang akan dikirim oleh user. Gambar 5 (b) menampilkan thread pesan SMS dari pengirim yang sudah terenkripsi.



(a) (b)

Gambar 5. (a)Tampilan popup kunci enkripsi; (b) Tampilan pesan yang sudah terenkripsi

Pada gambar 6 (a) menampilkan popup menu pilihan pesan. Menu message details yaitu menampilkan pengirim pesan, tanggal dan waktu dari pesan yang masuk. Menu forward untuk meneruskan atau mencopy semua pesan untuk dikirim kembali. Menu delete untuk menghapus pesan yang dipilih. Menu decrypt untuk mendekripsi pesan yang sudah terenkripsi dari pengirim. Gambar 6(b)menampilkan pesan yang sudah terdekripsi, sehingga dapat terbaca oleh user atau penerima.



(a) (b)

Gambar 6. (a) Tampilan menu pilihan pada pesan; (b) Tampilan popup pesan yang terdekripsi

KESIMPULAN

Berdasarkan hasil penelitian di atas, maka dapat disimpulkan bahwa sistem keamanan Short Message Service (SMS) berbasis android menggunakan algoritma Advanced Encryption Standard (AES) dapat mengirim SMS, dan memiliki fungsi merubah isi SMS menjadi chipertext agar isi informasi SMS tidak diketahui oleh orang lain.

DAFTAR PUSTAKA

[1] Subimawanto, Dami. Ihsani, Fuji. Hindharta, Jonathan. Pratama, Virgiawan Ananda Kamu, Melisa Chatrine. Pratama, Virgiawan Ananda. Rendianto, Muhammad, 2014. "Implementasi Algoritma Kriptografi Kode Caesar Vigenere, dan Transpososo untuk Sistem Proteksi Penggunaan Pesan Singkat (SMS) pada Smartphone Android", *Prosiding Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2014)*, Universitas Gunadarma, Depok.

[2] Soelistijanto, Bambang, 2010. "Implementasi Authentikasi Client dengan Metode Two Way Challenge Response pada Transaksi Perbankan Elektronik", *Seminar Nasional Informatika 2010*, UPN "Veteran" Yogyakarta, ISSN: 1979-2328.

[3] Wahyuni. Ana, 2011. *"Keamanan Pertukaran Kunci Kriptografi dengan Algortima Hybrid : Diffie-Hellman dan RSA"*, Fakultas Ilmu Komputer Universitas AKI.

[4] Rozidi,Romzi Imron, 2004. *"Membuat Sendiri SMS Gateway (ESME) Berbasis Protokol SMPP"*, Yogyakarta : Andi Offset.

[5] Sadikin ,Rifki, 2012. *"Kriptografi untuk Keamanan Jaringan",* Yogyakarta : Andi Offset.

[6] Kirat Pal Singh, dan Shiwani Dod, 2016. "An Efficient Hardware design and Implementation of Advanced Encryption Standard (AES) Algorithm", *International Journal of Recent Advances in Engineering & Technology (IJRAET).*

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

[8] M.Pitchaiah, Philemon Daniel, Praveen, 2012. "Implementation of Advanced Encryption Standard Algorithm", *International Journal of Scientific & Engineering Research*, Volume 3, Issue 3.