IMPLEMENTASI PENGAMANAN DATA ENKRIPSI SMS DENGAN ALGORITMA RC4 BERBASIS ANDROID

Sapto Subhan [1)], Safrina Amini [2)], Pipin Farida Ariyani [3)]

[1),2),3)]Teknik Informatika, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan
Email : safrina.amini@budiluhur.ac.id

Abstrak. *SMS merupakan suatu layanan yang diberikan oleh telepon selular kepada penggunanya untuk melakukan komunikasi melalui pengiriman pesan singkat dengan biaya yang murah. Kelebihan lainnya dari penggunaan SMS adalah pesan yang dikirimkan dapat diterima oleh penerima dengan baik dengan dukungan provider. Komunikasi melalui media SMS yang bukan komunikasi point-to-point menjadi salah satu kelemahan karena pesan yang dikirimkan melalui media SMS tidak langsung sampai pada tujuan, melainkan melalui jaringan SMS. Keamanan pesan dapat terancam untuk dibaca oleh orang yang tidak bertanggung jawab. Ancaman ini bisa diantisipasi dengan membangun perangkat lunak untuk meningkatkan keamanan pesan yang dikirim dengan melakukan enkripsi SMS. Metode pengamanan pesan dibangun dengan menggunakan algoritma RC4. Penggunanaan kunci privat dengan panjang yang beragam merupakan salah satu parameter dalam algoritma ini. Perangkat lunak dibangun menggunakan teknologi Java Android yang dapat ditanamkan pada telepon selular. Untuk bisa membaca pesan yang masuk, penerima harus melakukan deskripsi terlebih dahulu. Menu enkripsi dan dekripsi harus sudah ditanamkan pada telepon selular. SMS yang diterima tidak akan mengalami perubahan arti sehingga penerima tetap akan mendapatkan pesan yang tepat walaupun dalam pengiriman pesan sudah diamankan.*

Kata kunci*: SMS, enkripsi, dekripsi, RC4.*

1. Pendahuluan

1.1. Latar Belakang

Teknologi pada telepon seluler terus mengalami perkembangan. yang dahulu hanya dapat digunakan untuk melakukan panggilan dan mengirim pesan (SMS) kini dapat digunakan untuk berbagai macam hal seperti *chatting*, *browsing*, *video call*, dan lain lain. Meskipun demikian, layanan SMS masih tetap memiliki pengguna yang banyak. Dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS. Ada juga pengamanan SMS dengan menggunakan kriptografi SMS yang memanfaatkan kunci untuk medekripsikan SMS yang telah di enkripsi.

Kriptografi berbasis pada algoritma pengkodean data informasi yang mendukung kebutuhan dari dua aspek keamanan informasi, yaitu *secrecy* (perlindungan terhadap kerahasiaan data informasi) dan *authenticity* (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan).

Algortima RC4 (*Ron's Code 4*) adalah salah satu metode kriptografi yang sederhana dan cepat sehingga mudah diaplikasikan untuk pengamanan pesan. RC4 didesain oleh Ron Rivest yang berasak dari RSA Security. RC4 sendiri mempunyai singkatan resmi yaitu "*Rivest Chiper*". Rumusan permasalahan yang akan diselesaikan dalam penelitian ini adalah:

a. Bagaimana mengimplementasikan dan menerapkan algoritma kriptografi RC4?
b. Untuk pengamanan SMS bagaimanakah cara mengenkripsi dan mendekripsikannya kembali tanpa mengubah isi dari informasi tersebut?
c. Bagaimana perancangan aplikasi enkripsi SMS berbasis android dan fungsi-fungsi apa saja yang dibutuhkan?

Tujuan pembuatan aplikasi Enkripsi SMS dengan algoritma RC4 berbasis android adalah sebagai berikut :

a. Menggunakan cara pengimplementasian algoritma kriptografi RC4 kedalam bentuk aplikasi nyata.
b. Pengamanan SMS menggunakan cara enkripsi dengan algoritma kriptografi RC4 agar tidak dapat diketahui oleh orang yang tidak bersangkutan dan mendekripsikan kembali SMS tersebut.
c. Dengan rancangan yang baik akan menghasilkan aplikasi pengamanan SMS yang sesuai kebutuhan *user*.

Batasan masalah dalam pembuatan aplikasi SMS kriptografi menggunakan algoritma RC4 berbasis android yaitu:
a. Metode kriptografi yang digunakan adalah algoritma RC4.
b. Aplikasi ini dijalankan pada *smartphone* yang bersistem operasi android.
c. Bahasa pemrogaman yang digunakan adalah Java dan Xml.
d. Pembuatan aplikasi menggunakan editor Eclipse.
e. Aplikasi ini dibuat untuk mengamankan isi pesan SMS supaya tidak mudah dibaca.

Metodologi pengembangan sistem yang digunakan dalam penelitian ini adalah metode pengembangan model RAD (*Rapid Application Development*), Model ini dibuat untuk membuat sistem yang cepat tanpa harus mengorbankan kualitas. Dan melingkupi fase-fase sebagai berikut :
a. Fase Perencanaan
   Syarat-Syarat Pada tahap ini dilakukan penentuan tujuan dan syarat-syarat informasi.
b. Fase Perancangan
   Pada tahap ini dilakukan perancangan proses yaitu proses-proses yang akan terjadi di dalam sistem, yang terdiri dari perancangan proses dan perancangan antarmuka pemakai (*user interface*).
c. Fase Konstruksi
   Pada fase ini dilakukan tahap pengkodean terhadap rancangan-rancangan yang telah didefinisikan.
d. Fase Pelaksanaan
   Pada fase ini dilakukan pengujian terhadap sistem dan melakukan pengenalan sistem kepada pengguna.

1.2. Landasan Teori

SMS memiliki panjang isi pesan pada sebuah paket berukuran maksimal 160 karakter, dimana setiap karakter memiliki panjang 7 bit. Beberapa aplikasi standar telepon seluler dapat mendukung dengan panjang 8 bit (panjang maksimum 140 karekter) dan karakter yang lebih panjang lainnya seperti 16 bit, namun karekter sepanjang 8 bit dan 16 bit ini tidak didukung oleh semua apliaksi standar telepon genggam. Pada umumnya karakter sepanjang 8 bit dan 7 bit digunakan untuk menampilkan data seperti gambar dan simbol. Secara umum sebuah telepon genggam hanya dapat melakukan pengiriman satu buah paket SMS dalam satu pesan, namun dengan kemajuan teknologi sekarang SMS dikembangkan menjadi EMS *(Enhanched Message Service)* [1].
Algoritma pada dasarnya, adalah alur pikiran dalam menyelesaikan suatu pekerjaan, yang dituangkan dalam bentuk tertulis yand dapat dimengerti oleh orang lain [2].
Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Namun saat ini kriptografi lebih dari sekedar *privacy*, tetapi juga untuk tujuan data *integrity, authentication*, dan *non-repudiation* [3].
Dalam perkembangannya, kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan dan tanda tangan digital dan keaslian pesan dengan sidik jari digital [4]. Berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi 2 macam, yaitu algoritma simetri (*symetric algorithms*) dan algoritma asimetri (*asymetric algorithms)* [5].
Algoritma kriptografi Rivest Code 4 (RC4) merupakan salah satu algoritma kunci simetris yang berbentuk stream chipper. Algoritma ini ditemukan pada tahun 1978 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu: Rivest Shamir Adleman). RC4 menggunakan panjang kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte. Tabel ini digunakan untuk generasi yang berikut dari pseudo random yang menggunakan XOR dengan plainteks untuk menghasilkan cipherteks. Masing-masing elemen dalam tabel saling ditukarkan minimal sekali. RC4 merupakan salah satu jenis stream cipher sehingga RC4 memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya

sebuah byte atau bahkan kadang kadang bit (byte dalam hal RC4) sehingga dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkrip [6].

Aplikasi *mobile* berasal dari kata *application* dan *mobile*. *Application* yang artinya penerapan, lamaran, penggunaan. Secara istilah aplikasi adalah program siap pakai yang direka untuk melaksanakan suatu fungsi bagi pengguna atau aplikasi yang lain dan dapat digunakan oleh sasaran yang dituju sedangkan *mobile* dapat di artikan sebagai perpindahan dari suatu tempat ke tempat yang lain [7].

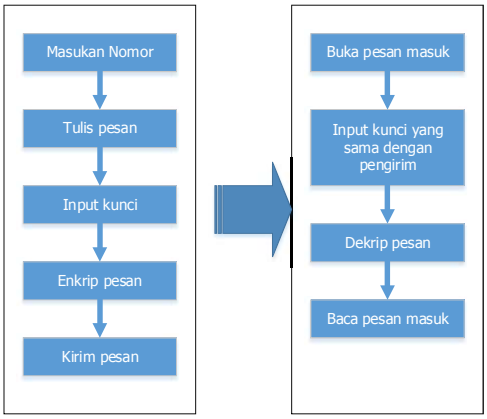
Android memiliki keamanan yang dirancang demi kenyamanan dari pengguna, namun beberapa layanan pada fitur-fitur tertentu yang sama sekali tidak memiliki metode pengamanan pada data yang disimpannya, salah satunya adalah layanan SMS (Short Massage Service) yang pada perangkat android secara default sama sekali tidak memiliki metoda pengamanan. Sehingga dibutuhkan untuk mengatasinnya software aplikasi pihak ketiga dalam mengamankan service SMS tersebut. Pengamanan atau security dari layanan penyedia SMS juga sangat perlu diperhatikan karena pengunaanya yang sangat dominan pada sebuah perangkat telepon dan juga memiliki celah keamanan yang besar yang mungkin menyebabkan datanya diketahui oleh pihak yang tidak dikehendaki. Android mendukung perkembangan yang cepat, karena seperti open source lainya android membuka code sumbernya secara gratis untuk dikembangkan oleh para developer [8].

2. Pembahasan

Permasalahan yang sedang dihadapi dan akan diimplementasikan pemecahannya adalah kurang terjaminnya kerahasiaan sebuah pesan yang dikirimkan. Upaya yang dilakukan adalah dengan berusaha mencari kombinasi teknologi hardware dan software yang tepat sehingga didapatkan hasil yang optimal dan mudah untuk diimplementasikan.

2.1. Deskripsi Rancangan Aplikasi

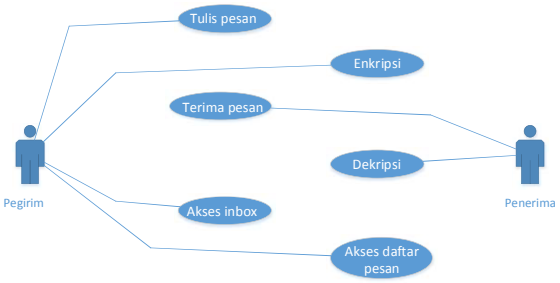
Pengguna akan berinteraksi dengan aplikasi melalui *user interface* yang tersedia, pengguna bisa membuat pesan terenkripsi ataupun membaca pesan yang terenkripsi. Pesan yang telah dibuat kemudian dikirimkan ke *smartphone* tujuan melalui jaringan SMS. Ketika pesan diterima oleh pengguna yang dituju, penerima harus menyamakan kunci untuk men-dekrip pesan apabila ingin membaca pesan yang diterima. Secara umum, rancangan aplikasi yang akan dibuat dapat dilihat pada Gambar 1 berikut ini:



Gambar 1. Rancangan umum aplikasi

2.2. Use Case Diagram Aplikasi

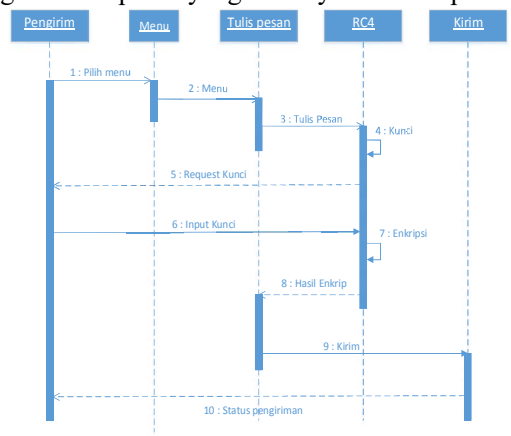
Berikut adalah *use case diagram* enkripsi dan dekripsi aplikasi SMS yang akan dibuat. *Use case* ini menjelaskan aktivitas antara pengirim dan penerima SMS, terlihat juga bahwa saat pesan akan dikirim terlebih dahulu pesan akan dienkripsi kemudian setelah sampai ke penerima pesan didekripsi agar terbaca dengan pesan sebenarnya.



Gambar 2. *Use case diagram* Aplikasi

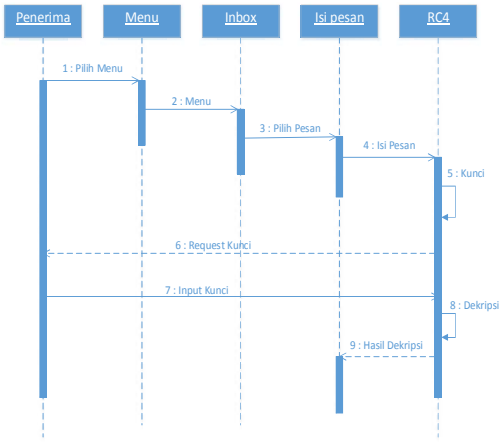
2.3. *Sequence* Diagram Aplikasi yang Akan Dibangun

Secara umum aplikasi ini terdiri dari dua bagian yang penting yaitu tulis pesan dan baca pesan. Berikut adalah *sequence* diagram tulis pesan yang nantinya akan terapkan dalam aplikasi SMS.



Gambar 3. *Sequence* diagram enkripsi dan pengiriman SMS

Kebalikan dari proses diatas, berikut ini adalah diagram baca pesan yang akan diterapkan dalam aplikasi berikut ini:



Gambar 4. *Sequence* diagram dekripsi SMS

2.4. Implementasi dan Uji Coba

Implementasi dan uji coba merupakan salah satu tahapan dalam pembuatan aplikasi. Pada pengimplementasian dan uji coba, akan dilakukan pengujian serta analisa dari aplikasi Enkripsi SMS dengan algoritma RC4 berbasis android yang telah dirancang. Tujuannya adalah untuk mengukur sejauh mana aplikasi ini dapat berjalan. Dengan adanya pengimplementasian serta uji coba tersebut, diharapkan aplikasi yang dibuat berjalan dengan baik dan siap dipakai. Sebelum melakukan percobaan atau implementasi pada aplikasi Enkripsi SMS dengan algoritma RC4 berbasis android *user* akan

melakukan instalasi pada smartphone. Setelah semua kebutuhan perangkat keras dan implementasi sistem dilakukan, selanjutnya adalah menguji proses enkripsi dan dekripsi. Berikut beberapa hasil analisis proses enkripsi dan dekripsi

Tabel 1. Percobaan enkripsi

No	plaintext	*Key* / Kunci	Ciphertext RC4
1	pesan enkripsi	89	14834BE8EC28D42DC47CD30E7EDED4B3
2	651 SMS Rahasia	key332	DA32BB64B96BF540A5DDD0B84A9285E5
3	Coba Enkripsi SMS	kunci private	236DB3D41CF9C66EB614610471DBE0B0BC08EE 9F0972564C078CB203A33EA89F

Tabel 2. Percobaan dekripsi kunci salah

No	Ciphertext RC4	*Key* / Kunci (salah)	Hasil Dekripsi Bila kunci salah
1	14834BE8EC28D42DC47CD30E7EDED4B3	uu	◆◆◆D◆◆6@◆ ◆◆m◆0
2	DA32BB64B96BF540A5DDD0B84A9285E5	345uyt	◆◆◆D◆◆6@◆ ◆◆m◆0
3	236DB3D41CF9C66EB614610471DBE0B0B C08EE9F0972564C078CB203A33EA89F	iop88	◆2 En◆◆g ◆◆ A◆ 3◆◆◆~ ~g:

Tabel 3. Percobaan dekripsi kunci benar

No	Ciphertext RC4	*Key* / Kunci (Benar)	Hasil dekripsi bila kunci benar
1	14834BE8EC28D42DC47CD30E7EDED4 B3	89	pesan enkripsi
2	DA32BB64B96BF540A5DDD0B84A9285 E5	key332	651 SMS Rahasia
3	236DB3D41CF9C66EB614610471DBE0B 0BC08EE9F0972564C078CB203A33EA89 F	kunci private	Coba Enkripsi SMS

Dari hasil percobaan terhadap proses enkripsi dan proses dekripsi yang telah Dilakukan, dapat diambil kesimpulan bahwa aplikasi telah melakukan proses enkripsi dan dekripsi dengan baik. Semua pesan yang telah dikirim dalam bentuk cipher dapat diterima dan didekripsi kembali tanpa adanya kesalahan dengan memasukan kunci yang benar atau sama.

2.5. Kelebihan aplikasi

a. Faktor keamanan pada pengiriman SMS dengan *smartphone* android lebih terjamin kerahasiaanya.
b. Aplikasi mudah untuk digunakan sama hal-nya seperti aplikasi pengirim SMS lainnya.
c. Enkripsi dengan kunci yang salah akan membuat pesan semakin sulit terbaca.
d. Penggunaan algoritma RC4 menambah tingkat keamanan, karena pesan akan dienkripsi

2.6. Kekurangan aplikasi

a. Belum adanya fitur *outbox* dimana fitur ini menampilkan semua pesan keluar.
b. Tidak tersedianya fitur balas SMS terhadap SMS yang masuk.
c. Semakin panjang isi pesan maka semakin panjang pula hasil enkripsinya.
d. Aplikasi tidak memiliki fitur untuk melakukan manajemen kunci, sehingga harus menginput kunci yang berbeda jika ingin berpesan SMS.
e. SMS tidak terintegrasi dengan kontak, berbeda dengan aplikasi SMS default android.
f. Aplikasi belum bisa mengirim dan menerima file gambar ataupun audio (MMS) terenkripsi.

3. Simpulan

Setelah beberapa melewati tahap perancangan dan uji coba aplikasi enkripsi SMS dengan algoritma RC4, ada beberapa kesimpulan yang dapat diambil. Sehingga dalam penggunaan aplikasi ini diharapkan dapat membantu untuk memberikan solusi dari masalah yang ada dengan pertimbangan sebagai berikut:

a. Algoritma RC4 dapat digunakan untuk mengenkrip SMS dan dapat juga mendekrip SMS menggunakan kunci yang sesuai atau sama.
b. Pengamanan SMS dengan algoritma RC4 dapat digunakan untuk menjaga kerahasiaan pesan yang dikirim.
c. Panjang hasil enkripsi RC4 bisa lebih panjang dari teks aslinya.

Aplikasi enkripsi SMS ini masih jauh dari sempurna dan masih sangat diperlukan pengembangan dan bermacam perbaikan yang ditujukan untuk dapat memnerikan kemudahan bagi penggunanya lebih lanjut dengan beberapa perkembangan lagi, antara lain:

a. Aplikasi ini belum ada fitur untuk melakukan manajemen kunci enkripsi dan dekripsi, dan fitur ini diharapkan ada pada pengembangan selanjutnya.
b. Penambahan fitur *inbox* dan *outbox* menjadi satu yang terintegrasi dengan kontak, sehingga lebih memudahkan pengguna dalam mengirim dan menerima pesan.
c. Penambahan enkripsi untuk mengirim dan menerima pesan gambar atau audio terenkripsi.

Daftar Pustaka

[1] Zakaria, Marcus, 2013. Aplikasi SMS Untuk Berbagai Keperluan, Bandung, Informatika. 1998.
[2] Sjukani.Moh, 2011. Algoritma Struktur 1 Edisi Tujuh, Jakarta, Mitra Wacana Media, hal 1.
[3] Munir, Rinaldi 2005. Kriptografi, Bandung, Informatika.
[4] Ariyus, Dony 2005. Computer Security, Yogyakarta, Andi.
[5] Ariyus, Dony 2006. Kriptografi, Keamanan Data dan Komunikasi, Yogyakarta, Graha Ilmu.
[6] Yuri Ariyanto, Jurusan Teknik Informatika Jurnal Informatika Vol.10, No.1, Mei 2009, "ALGORITMA RC4 DALAM PROTEKSI TRANSMISI DAN HASIL QUERY UNTUK ORDBMS POSTGRESQL".
[7] Buyens, Jim, 2001. Web Database Development, Jakarta, Elex Media Komputindo.
[8] Rahmayun, Indri & Defni, Jurnal Momentum Vol.16, No.1, Februari 2014, ISSN : 1693-752X, "ENKRIPSI SMS (SHORT MESSAGE SERVICE) PADA TELEPON SELULAR BERBASIS ANDROID DENGAN METODE RC6".