

APLIKASI KRIPTOGRAFI DALAM MENGAMANKAN PESAN TEKS DENGAN METODE ALGORITMA RC4 BERBASIS ANDROID

ROSNA DEWI, T.M¹, JOHAN, M.IT², IMAM MUSLEM R, ST, M.Kom³

Address: Mahasiswa Teknik Informatika, Fakultas Ilmu Komputer, Universitas Almuslim, Dosen Teknik Informatika, Fakultas Ilmu Komputer, Universitas Almuslim, Jalan Almuslim No. 1, Bireuen-Aceh Indonesia

Email: ratnadewi0976@gmail.com^{1*}

Abstrak

Perkembangan teknologi telekomunikasi pada saat ini semakin canggih sehingga dapat membantu kegiatan sehari-hari. Salah satu contoh media komunikasi *short service message* (SMS), yang dapat melakukan berbagai teknik pengambilan informasi baik legal maupun illegal. Berbagai teknik perlindungan informasi yang dirahasiakan dari yang tidak berhak telah dikembangkan untuk melindungi informasi. Kriptografi adalah teknik penulisan pesan rahasia agar orang tidak dapat mengetahui. Algoritma RC4 adalah salah satu teknik yang digunakan untuk membuat pesan rahasia dengan teknik enkripsi dan dekripsi pesan. Penelitian ini bertujuan untuk merancang suatu aplikasi kriptografi dalam pengamanan pesan teks, yang diimplementasikan pada perangkat *mobile* berbasis android. Aplikasi ini dikembangkan dengan aplikasi *eclipse* dan teknik kriptografi yang dikembangkan dengan algoritma *Rivest Code 4* (RC4).

Keywords Kriptografi, Algoritma RC4, Android

I. PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi telekomunikasi, maka semakin berkembang pula ilmu kriptografi baik jenis maupun fungsinya. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Namun dalam kenyataannya kadang hal ini bertolak belakang. Masalah keamanan kurang mendapat perhatian dari perancang dan pengelola sistem informasi. Hal sering terjadi malah keamanan berada di urutan terakhir dalam hal-hal yang dianggap penting, setelah urusan tampilan. Sebuah organisasi yang baik dilihat dari kemampuannya untuk menyediakan informasi secara cepat dan tepat. Hal ini menjadi sangat mungkin untuk saat ini terutama dengan semakin berkembangnya teknologi komputer dan telekomunikasi.

Dalam kehidupan sehari-hari manusia banyak bergantung pada teknologi informasi, baik dari hal kecil hingga ke permasalahan yang rumit. Kemajuan

teknologi informasi memberikan banyak keuntungan bagi kehidupan manusia. Tetapi keuntungan yang ditawarkan oleh teknologi informasi juga menimbulkan kejahatan seperti pencurian data. Keamanan data merupakan sesuatu yang harus diperhatikan dalam kemajuan teknologi informasi, terutama dalam pesan yang berbentuk teks.

Salah satu pencegahan yang dapat dilakukan adalah menggunakan aplikasi berbasis kriptografi. Banyak orang yang merasa asing dengan kata kriptografi, padahal kata ini sering digunakan dalam penggunaan jaringan komputer. Menurut terminologinya, kriptografi adalah ilmu atau seni untuk menjaga keamanan pesan, ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi dari pesan tersebut kemungkinan dapat disadap oleh pihak lain. Untuk menjaga keamanan pesan, maka pesan tersebut dapat di-*scramble* / diacak atau diubah menjadi kode yang tidak dapat dimengerti oleh orang lain. Tujuan utama sistem kriptografi adalah

mengamankan informasi yang bersifat rahasia serta menjaga keutuhan informasi tersebut.

Berdasarkan uraian di atas, maka penulis mengangkat masalah ini dalam Skripsi dengan judul. "Aplikasi Kriptografi Dalam Mengamankan Pesan Teks Dengan Metode Algoritma RC4 Berbasis Android".

1.2 Rumusan Masalah

- Bagaimana membuat aplikasi enkripsi untuk mengamankan pesan teks dengan menggunakan algoritma RC4?
- Bagaimana proses penyandian serta implementasi dari algoritma RC4?
- Bagaimana merancang suatu program yang dapat membantu implementasi aplikasi kriptografi dalam mengamankan pesan teks dengan metode algoritma RC4 berbasis Android?

1.3 Batasan Masalah

- Metode algoritma yang dipakai adalah RC4.
- Data yang disandikan adalah data teks.
- Program dirancang menggunakan sistem operasi Android.

1.4 Tujuan Penelitian

Untuk membuat suatu perangkat lunak aplikasi kriptografi dalam mengenkripsi pesan teks dengan menggunakan metode algoritma RC4 serta cara mengimplementasikannya di sistem operasi yang berbasis Android.

1.5 Manfaat Penelitian

- Bagi Penulis, membantu pemahaman tentang kriptografi terutama mengenai algoritma RC4 dan menambah pengetahuan penulis mengenai pembuatan perangkat lunak aplikasi kriptografi dalam mengamankan pesan teks dengan metode algoritma RC4 berbasis Android sebagai bahan perbandingan antara teori yang diperoleh dengan praktek yang sebenarnya.
- Bagi Pembaca, Menambah pengetahuan tentang aplikasi kriptografi dalam mengamankan pesan teks dengan metode algoritma RC4 berbasis Android dan diharapkan dapat bermanfaat dan dapat

dipertimbangkan untuk dapat dikembangkan di masa yang akan datang.

1.6 Metodologi Penelitian

Adapun metodologi yang digunakan adalah sebagai berikut:

- Pengumpulan data, dilakukan dengan mencari informasi bahan masakan dan cara membuat masakan khas aceh dari buku resep masakan dan dari internet.
- Perencanaan, pada tahapan ini dilakukan dengan perancangan tampilan disetiap halaman untuk aplikasi.
- Pembuatan program/ coding, dalam pembuatan program aplikasi ini menggunakan *software* Android Studio untuk pemrograman pembuatan aplikasi.
- Uji coba aplikasi, untuk dapat menjalankan aplikasi resep masakan dibutuhkan emulator sebagai perangkat lunak, yaitu AVD manager, yang selanjutnya aplikasi disiapkan dalam paket guna dapat di install pada perangkat mobile android untuk pengujian.
- Pemeliharaan, pada bagian ini aplikasi resep masakan yang telah dibuat dilakukan pemeliharaan untuk keutuhan aplikasi guna menghindarkan kemungkinan adanya gangguan dari sistem atau sebagainya.

II. LANDASAN TEORI

Kriptografi (*cryptography*) berasal dari bahasa Yunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia) (Munir, 2006).

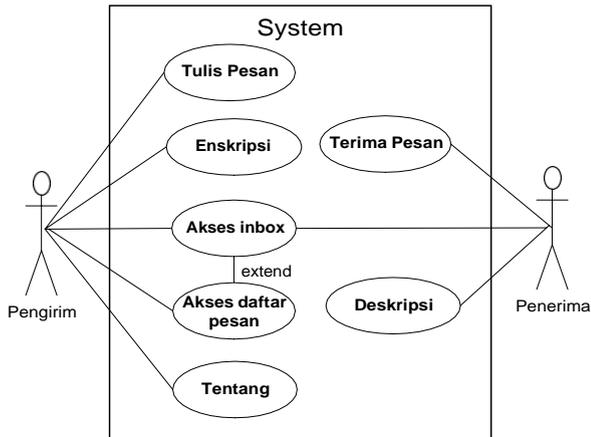
Ada banyak model dan metode enkripsi, salah satu di antaranya adalah enkripsi dengan algoritma *Rivest Code 4* (RC4). Model ini merupakan salah satu algoritma kunci simetris yang berbentuk *stream chipper*, artinya operasi enkripsi dilakukan per karakter 1 byte untuk sekali operasi (Jamaluddin, 2010).

Menurut Nasruddin Safaat (2012) menjelaskan bahwa "android adalah sebuah sistem operasi pada handphone yang bersifat terbuka dan berbasis pada sistem operasi Linux".

Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya (Dadan Rosnawan, 2011).

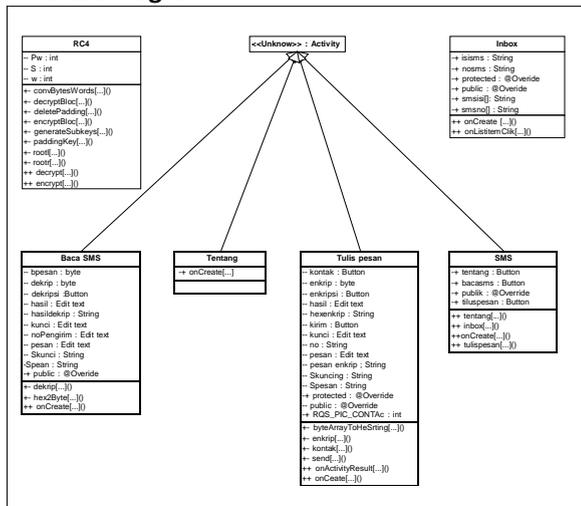
III. PERANCANGAN

3.1 Use Case Diagram



Gambar 3.1. Use casediagram

1.2 Class Diagram



Gambar 3.2 Class diagram

IV. IMPLEMENTASI

4.1 Pengujian Aplikasi

Pengujian yang dilakukan dengan menguji dengan meng-*compile* program agar dapat berjalan dalam *emulator* dan mem-*package* aplikasi dalam bentuk *file* apk untuk dapat diinstallkan pada *smartphone* atau perangkat seluler lainnya yang mempunyai *operating system(OS) android*.

Berdasarkan hasil pengujian dengan kasus *sample* uji yang telah dilakukan maka hasil pengujian dapat memberikan kesimpulan bahwa aplikasi sistem informasi geografis pemetaan polindes berbasis

android dapat berjalan dengan baik dan sesuai kebutuhannya dan juga dapat menghasilkan *output* yang diharapkan.

Meski pengujian yang dilakukan masih terbilang minimal namun perangkat lunak bebas dari kesalahan sintak dan secara fungsional dapat mengeluarkan hasil yang sesuai dengan yang diharapkan dan sudah dapat mewakili pengujian fungsionalitas yang lainnya, adapun hasil pengujian adalah sebagai berikut :



Gambar 4.1 Pengujian spals screen



Gambar 4.2 Pengujian menu utama



Gambar 4.3 Pengujian menu enkripsi



Gambar 4.4 Pengujian menu dekripsi



Gambar 4.5 Pengujian menu tentang



Gambar 4.6 Pengujian menu keluar

V. KESIMPULAN

5.1 Kesimpulan

Berdasarkan bahasan dari keseluruhan bab dalam skripsi ini, adapun kesimpulan dari skripsi adalah sebagai berikut :

- Aplikasi yang dibuat adalah untuk pengamanan atau kriptografi dalam mengamankan pesanteks berbasis android
- Algoritma yang digunakan adalah algoritma *Rivesrt Code (RC4)* dibuat sesuai dengan pengembangan sistem berdasarkan permasalahan serta analisa sistem untuk pesan teks.
- Aplikasi ini dibuat sebagai sebuah aplikasi *mobile android* yang dipergunakan untuk kriptografi, dengan menggunakan fasilitas sms dari *smartphone* berbasis android.

5.2 Saran

Adapun saran agar aplikasi ini bisa berfungsi dengan baik lebih *optimal* dan lebih menarik semisalnya pada desain *interface* (antarmuka) dapat diberikan tampilan yang lebih menarik dan *interaktif* serta menu-menu interaktif lainnya, serta menambahkan lebih banyak fitur menu, untuk proses kriptografi, terutama dalam proses kriptografi,

UCAPAN TERIMA KASIH

Ucapan terimakasih tak lupa pula penulis hanturkan kepada berbagai pihak yang telah membantu baik secara material maupun moral atas dukungan-dukungan maupun bimbingan-bimbingan sehingga penulis dapat menyelesaikan skripsi ini, terutama kepada :

- Kepada kedua orang tua penulis yang telah bersusah payah membesarkan penulis dengan kasih sayang dan membimbing ke ilmu pengetahuan yang baik sehingga penulis dapat menyelesaikan pendidikan ini.
- Kepada sanak saudara adik-adik penulis yang kusayangi atas semangat dan motivasinya dalam memberikandukungan.
- Rektor Universitas Almuslim Kabupaten Bireuen Bapak H. DR Amiruddin Idris, SE, M.Msi.
- Bapak Taufik ST, MT selaku Dekan Fakultas Ilmu Komputer Universitas Almuslim.
- Bapak T.M Johan, M.IT dan Imam Muslem R, ST, M.kom selaku pembimbing I dan pembimbing II yang telah mau meluangkan waktu dan kesempatan guna memberikan bimbingan kepada penulis sehingga dapat menyelesaikan penulisan skripsi ini.
- Para Dosen dan staf akademik Fakultas Ilmu Komputer Universitas Almuslim atas perhatiandan dukungannya.

7. Rekan dan sahabat mahasiswa dan mahasiswi sekalian seperjuangan atas dukungan dan motivasinya, dan semua pihak yang berpartisipasi atas penyelesaianpenuliskripsiini.

Atas semua dukungan dan do'a yang telah diberikan penulis senantiasatidak dapat membalasnya selain mengucapkan syukur dan terima kasih, moga Allah SWT memberikan balasan yang baik serta senantiasaselalu dalam lindungan dan rahmat-Nya.

DAFTAR PUSTAKA

- [1]. Abdurachman, Harry, dkk, (2015), *Keamanan Komu-nikasi Data Sms Pada Android Den-gan Menggunakan Aplikasi Kriptogra-pi Advance Encryption Standard (AES)*, <http://jurnal.sttgarut.ac.id>, diakses tanggal 28 Januari 2016.
- [2]. Ardiansyah, F, 2011, *Pengenalan Dasar Android Programming*, Birainara, Depok
- [3]. Haryanto, B, 2004, *Rekayasa Sistem Berorientasi Objek*, Informatika, Bandung
- [4]. Huda, Akbarul. A, 2012, *Live Coding, Edisi 1*, Andi Yogyakarta, Yagyakarta
- [5]. Huda, Akbarul. A, 2013, *Live Coding9 Aplikasi Android Buatan Sendiri*, Andi Yogyakarta, Yogyakarta
- [6]. Irawan, F, H, (2013), *Sistem Keamanan Pesan Pada Android Gingerbread (2.3.4) Dengan Algoritma LUC*, <http://repository.unej.ac.id>, diakses tanggal 28 Januari 2016.
- [7]. Khannedy, K.E, 2012, *Membuat Aplikasi Android Sederhana*, Strib Bandung, Bandung
- [8]. Lubis, B, S, (2013), *Aplikasi enkripsi SMS (Short Message Service) Menggunakan Algoritma Data Encryption Standard (DES) Berbasis Android*, <http://pelita-informatika.com>, diakses tanggal 28 Januari 2016.
- [9]. Murya, Y, 2014, *Pemograman Android Blackbox*, Jasakom, Jakarta
- [10]. Nugroho, B, 2004, *Rekayasa Sistem Berorientasi Objek*, Informatika, Bandung.
- [11]. Putra, Arthdi. A, 2012, *Androiddan Anak Tukang Sayur Buku Praktis Belajar Pemograman Android*, Edisi 1.0, Stackoverflow, Lubuklinggang.
- [12]. Sammerville, 2013, *Software Engineering (Rekayasa Perangkat Lunak), Jilid 2*, Erlangga, Jakarta.
- [13]. Sholiq, 2006, *Permodelan Sistem Berorientasi Objek dengn UML*, Graha Ilmu, Yogyakarta.
- [14]. Siallagan, S, 2009, *Pemrograman Java dasar-dasar Pengenalan dan Pemahaman*, Andi Yogyakarta, Yogyakarta