RANCANG BANGUN APLIKASI ENKRIPSI SMS BERBASIS ANDROID MENGGUNAKAN ALGORITMA BLOWFISH

Ardi Mardiana[1], Ade Bastian[2], Enjen Saenudin[3]
[1,2,3] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Majalengka
e-mail: [1]aim@ft.unma.ac.id, [2]adb@ft.unma.ac.id, [3]zenc007@gmail.com

ABSTRAK

Beberapa tahun terakhir ini terjadi perkembangan yang pesat pada teknologi, salah satunya adalah telepon selular (ponsel). Berbagai perangkat lunak untuk mengembangkan aplikasi ponselpun bermunculan, diantaranya yang cukup luas adalah android. Meskipun pesatnya perkembangan smartphone beserta operating system namun layanan pesan singkat (SMS) melalui ponsel masih digunakan oleh masyarakat. Namun dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS. Seiring dengan perkembangan teknologi saat ini muncul pula permasalahan yang berhubungan dengan tingkat keamanan layanan tersebut. Kemudahan pertukaran informasi melalui SMS disalahgunakan oleh sebagian orang dengan berbagai cara mencoba untuk mencuri informasi.

Sebab itu dibutuhkan pengamanan informasi yang kita kirimkan melalui layanan SMS, dengan mengembangkan perangkat lunak yang berfungsi sebagai aplikasi SMS kriptogarfi yang mampu melakukan proses enkripsi dan dekripsi SMS pada smartphone berbasis android dengan menggunakan algoritma blowfish.

***Kata Kunci**: Enkripsi, SMS, Android, Algoritma, Blowfish*

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini membawa cara berkomunikasi yang beragam bagi manusia dengan munculnya berbagai macam media komunikasi untuk bertukar informasi. Telepon selular merupakan media berkomunikasi yang umum digunkan manusia sekarang ini karena memberikan kemudahan bagi penggunanya dalam berkomunikasi lisan maupun tulis.

Berbagai perangkat lunak untuk mengembangkan aplikasi ponselpun bermunculan, diantaranya yang cukup luas adalah android. Meskipun pesatnya perkembangan smartphone beserta operating system namun layanan pesan singkat (SMS) melalui ponsel masih digunakan oleh masyarakat. SMS merupakan salah satu fasilitas yang disediakan ponsel untuk melakukan pengiriman data berupa pesan singkat. Namun dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS. Seiring dengan perkembangan teknologi saat ini muncul pula permasalahan yang berhubungan dengan tingkat keamanan layanan tersebut. Kemudahan pertukaran informasi melalui SMS disalahgunakan oleh sebagian orang dengan berbagai cara mencoba untuk mencuri informasi.

Berangkat dari permasalahan Metta Dharmasaputra mengenai penyadapan pesan singkatnya (SMS) dengan Vincentius Amin Sutanto, para wartawan Indonesia sepatutnya berhati-hati saat melakukan komunikasi dengan narasumber. Metta yang bukan seorang pelaku tindak pidana, teroris, dan pengedar narkotika (sesuai Nomor 36 Tahun 1999 tentang Telekomunikasi dan Peraturan Pemerintah Nomor 52 Tahun 2000) ternyata bisa disadap, itu berarti hal serupa bisa terjadi pada siapa saja. PT Telekomunikasi Indonesia Tbk. (Telkom) mengakui telah memberikan salinan sms Metta kepada penegak hukum, namun kepala Polri justru membantah telah memerintahkan penyadapan pesan singkat tersebut. Sedangkan menurut Ajun Komisaris Besar Aris Munandar, Kepala Satuan Fiskal Moneter dan Devisa Direktorat Reserse Kriminal Khusus Kepolisian Daerah Metro Jaya, meminta rekaman percakapan lewat pesan singkat itu sesuai dengan undang-undang untuk kebutuhan penyidikan. Padahal jelas penyadapan terhadap segala bentuk percakapan baru bisa dilaksanakan setelah ada penetapan pengadilan.

2. TINJAUAN PUSTAKA

2.1 Kriptografi

Kata kriptografi berasal dari bahasa Yunani, "kryptós" yang berarti tersembunyi dan "gráphein" yang berarti tulisan. Sehingga kata kriptografi dapat diartikan berupa frase "tulisan tersembunyi". Menurut Request for Comments (RFC), kriptografi merupakan ilmu matematika yang berhubungan dengan transformasi data untuk membuat artinya tidak dapat dipahami (untuk menyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah. Jika transformasinya dapat dikembalikan, kriptografi juga bisa diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang dapat dipahami. Artinya, kriptografi dapat diartikan sebagai proses untuk melindungi data dalam arti yang luas [1].

Dalam kamus bahasa Inggris Oxford diberikan pengertian kriptografi sebagai berikut :

"Sebuah teknik rahasia dalam penulisan, dengan karakter khusus, dengan menggunakan huruf dan karakter di luar bentuk aslinya, atau dengan metode-metode lain yang hanya dapat dipahami oleh pihak-pihak

yang memproses kunci, juga semua hal yang ditulis menggunakan cara seperti ini." Jadi, secara umun dapat diartikan sebagai seni menulis atau memecahkan cipher [2].

2.2 Algoritma Blowfish

Blowfish merupakan metoda enkripsi yang mirip dengan DES (DES-like cipher) dan diciptakan oleh Bruce Schneier yang ditujukan untuk mikroposesor besar (32 bit ke atas dengan cache data yang besar). Blowfish dikembangkan untuk memenuhi kriteria disain sebagai berikut:

a. Cepat, pada implementasi yang optimal Blowfish dapat mencapai kecepatan 26 clock cycle per byte.
b. Kompak, Blowfish dapat berjalan pada memori kurang dari 5 KB.
c. Sederhana, Blowfish hanya menggunakan operasi yang simpel: penambahan (addition), XOR, dan penelusuran tabel (table lookup) pada operand 32 bit. Desainnya mudah untuk dianalisa yang membuatnya resisten terhadap kesalahan implementasi.
d. Keamanan yang variabel, panjang kunci Blowfish dapat bervariasi dan dapat mencapai 448 bit (56 byte).

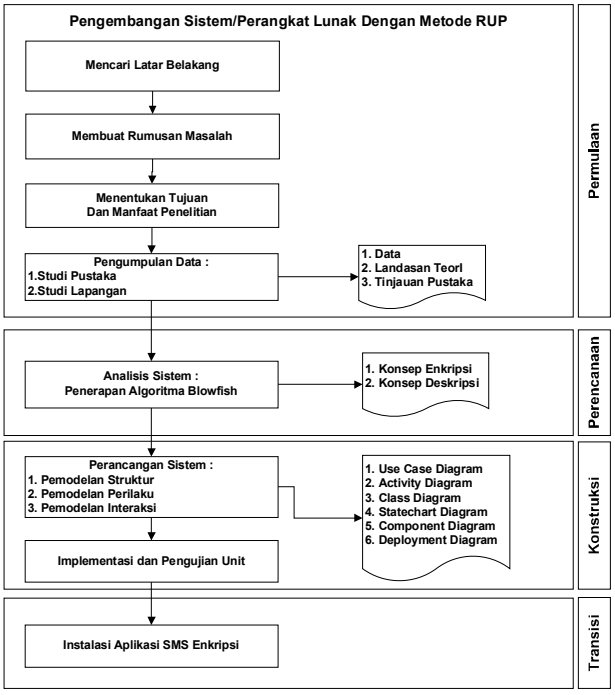
Blowfish dioptimasikan untuk aplikasi dimana kunci tidak sering berubah, seperti jalur komunikasi atau enkripsi file otomatis. Blowfish jauh lebih cepat dari DES bila diimplementasikan pada 32 bit mikroprosesor dengan cache data yang besar, seperti Pentium dan Power PC, Blowfish tidak cocok untuk aplikasi seperti packet switching, dengan perubahan kunci yang sering, atau sebagai fungsi hash satu arah. Kebutuhan memorinya yang besar tidak memungkinkan untuk aplikasi kartu pintar (smart card).

3. METODE PENELITIAN

3.1 Kerangka Penelitian

Kerangka pemikiran merupakan suatu diagram yang menjelaskan secara garis besar alur logika berjalannya sebuah penelitian. Kerangka pemikiran dibuat berdasarkan pertanyaan penelitian (research question), dan merepresentasikan suatu himpunan dari beberapa konsep serta hubungan diantara konsep-konsep tersebut.

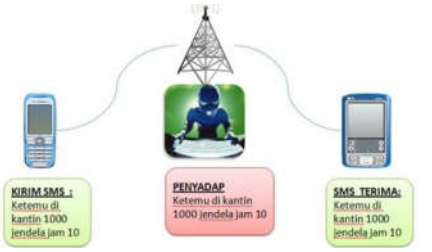
Adapun fungsi penyusunan kerangka penelitian adalah untuk memperoleh kesimpulan dari hasil penyelesaian suatu permasalahan. Berikut ini merupakan kerangka penelitian rancang bangun aplikasi SMS enkripsi.



Gambar 1. Kerangka Penelitian

3.2 Analisis Algoritma Blowfish

Secara default, SMS dikirim dalam bentuk plain text (meskipun di encoding/decoding dengan PDU) tanpa terenkripsi dari pengirim ke penerima SMS. Jika ada sniffing/penyadapan di jalur komunikasi, maka teks SMS akan sangat mudah dibaca oleh penyadap.

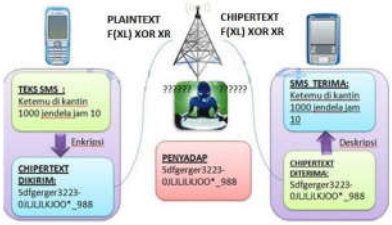


Gambar 2. Proses Komunikasi Tanpa Aplikasi Kriptografi

Dari Gambar 2 tersebut maka diperlukan sebuah aplikasi yang bisa mengenkripsi SMS yang akan dikirim, menjadi chipertext dengan algoritma kriptografi yaitu algoritma blowfish. Sehingga Teks SMS yang lewat pada jalur komunikasi dan masuk ke operator seluler adalah dlm bentuk chipertext(susah ditebak isi SMSnya). Pada penerima SMS, dilakukan Deskripsi teks SMS yang berupa chipertext sehingga bisa dibaca secara normal oleh penerima SMS.

Contoh kasus :

Gambar 3 adalah contoh penerapan algoritma blowfish aplikasi SMS kriptografi pada Android.

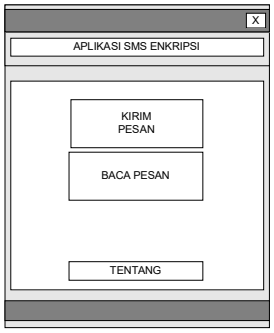


Gambar 3. Penerapan Algoritma Blowfish Aplikasi SMS Kriptografi

4. HASIL DAN PEMBAHASAN

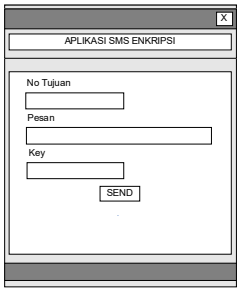
4.1 Rancangan Tampilan

Untuk memudahkan dalam pembuatan aplikasi, sebelumnya dibuat rancangan tampilan memuat fitur-fitur yang tersedia di dalam aplikasi SMS Kriptografi. Pada Gambar 4 rancangan tampilan Aplikasi SMS Kriptografi terdiri dari menu kirim pesan, baca pesan dan tentang.



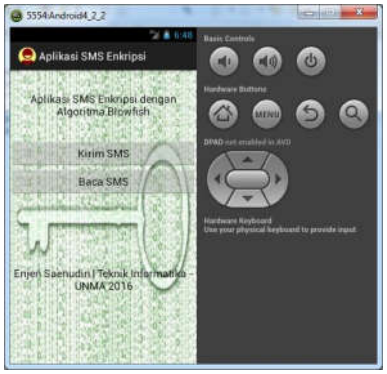
Gambar 4. Rancangan Tampilan Muka Aplikasi SMS Kriptografi

Setelah merancang tampilan muka, maka dirancang pula tampilan dalam Aplikasi SMS kriptografi. Gambar 5 menunjukkan tampilan untuk mengirimkan pesan. Kolom yang disiapkan antara lain nomor telepon, isi pesan dan kunci dari pesan.

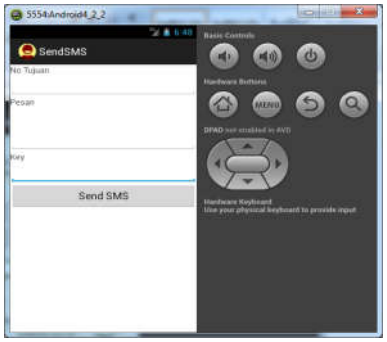


Gambar 5. Rancangan Tampilan Kirim Pesan Aplikasi SMS Kriptografi

Seletah mempunyai dasar untuk perancangan tampilan Aplikasi SMS Kriptografi, selanjutnya dilakukan pembuatan Aplikasi SMS Kriptografi. Tampilan akhir hasil perancangan ada pada Gambar 6 dan Gambar 7.



Gambar 6. Antar Muka Aplikasi SMS Kriptografi



Gambar 7. Antar Muka Kirim Pesan Aplikasi SMS Kriptografi

5. KESIMPULAN

Dari uraian yang terdapat pada laporan ini, maka penulis menarik beberapa kesimpulan sebagai berikut:

a. Dengan rancang bangun aplikasi enkripsi sms (short message service) pada telepon selular berbasis android dengan menggunakan algoritma blowfish setiap orang dapat mengamankan pesan informasinya yang bersifat rahasia baik yang dikirim maupun yang diterima dalam bentuk sms.
b. Rancangan arsitektur aplikasi enkripsi sms (short message service) ini menggunakan teknologi yang mendukung platform android dengan menggunakan bahasa pemrograman java android sehingga aplikasi yang dihasilkan dapat diterapkan pada telepon selular berbasis android.
c. Dengan menggunakan algoritma blowfish maka pesan sms akan lebih aman karena diterapkan proses enkripsi dan deskripsi.
d. Dengan aplikasi yang dapat diterapkan pada smartphone berbasis android maka setiap orang akan lebih mudah menggunakan aplikasi ini.

DAFTAR PUSTAKA

[1] Oppliger Rolf. 2005. Contemporary Cryptography. USA: Artech House, Inc.
[2] Talbot, Jhon dan Dominic Welsh. 2006. Complexity and Cryptography. USA : Cambridge University Press