

BAB I

PENDAHULUAN

1.1 Latar Belakang

Komunikasi merupakan kegiatan untuk menyampaikan sebuah informasi kepada orang lain, semakin berkembangnya zaman semakin berkembang juga cara-cara penyampaian komunikasi. SMS merupakan salah satu cara untuk menyampaikan informasi, perkembangan SMS saat ini yaitu *instant messenger*, *instant messenger* merupakan suatu system peniriman pesan yan instant dengan memanfaatkan jaringan internet.

Berbicara tentang jaringan internet, semakin lama perkembangan ponsel juga ikut berkembang menyesuaikan perkembangan jaringan internet seperti munculnya *smartphone*, *smartphone* yang ada saat ini sangat beragam jenis dan sistem operasinya. *Smartpone* sangat mendukung untuk aplikasi-aplikasi *instant messenger*, berdasarkan survei sistem operasi android merupakan sistem operasi yang paling banyak digunakan di Indonesia dibandingkan dengan sistem operasi lain seperti iOS, Symbian, BlackBerry OS, dll, namun pada *smartphone* dengan berbagai macam sistem operasi pasti terdapat fitur bawaan untuk menyampaikan pesan yaitu SMS.

Berdasarkan survei yang dirilis oleh Ofcom, khususnya di Indonesia *instant messenger* lebih digunakan dibandingkan dengan SMS, namun penurunan penggunaan SMS di Indonesia tidak drastis, pada tahun 2011 tercatat 250miliar pesan per tahun, kemudian pada tahun 2014 menurun menjadi 210 miliar per tahun.

Perbedaan SMS dan *intant messenger* selain sistem pembayaran pengiriman pesan adalah tingkat keamanan dalam pengiriman pesan. Pada layanan SMS masih memiliki kekurangan salah satunya, kurangnya keamanan dalam penyampaian pesan dikarenakan pesan yang dikirim akan dikirim apa adanya sesuai dengan yang telah diketikkan oleh pengirim, hal ini dapat mengakibatkan bocornya informasi yang dikirim, seandainya pada saat pengiriman ada seseorang yang menyadap jaringan komunikasi tersebut.

Kemudian layanan SMS dibatasi hanya dapat mengirim 160 karakter setiap sekali pengiriman, jika mengirim lebih dari 160 karakter maka akan dikenakan biaya tambahan, oleh sebab itulah peneliti melakukan penelitian ini untuk mengatasi dua masalah yang telah disebutkan yaitu: keamanan dan pemampatan pesan, sehingga pesan yang dikirim tidak dapat dibaca secara langsung oleh orang yang tidak berhak tanpa kunci keamanan, dan pesan yang akan dikirim dimampatkan sedemikian sehingga dapat mengurangi biaya pengiriman SMS.

Untuk mengamankan pesan, kriptografi adalah salah satu solusinya, kriptografi berasal dari bahasa Yunani yaitu *Crypto* yang berarti rahasia, dan *Graphen* yang berarti tulisan, sehingga kriptografi adalah metode untuk menyamarkan (merahasiakan) isi dari data sehingga tidak mudah untuk dibaca oleh orang yang tidak berhak untuk membacanya.

Metode kriptografi yang akan digunakan adalah RSA, metode RSA adalah metode kriptografi asimetrik key, yaitu metode ini mempunyai dua buah kombinasi kunci untuk enkripsi (*public key*) dan dekripsi (*private key*), RSA diciptakan oleh mahasiswa MIT pada tahun 1976 yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman, kerumitan metode ini terletak pada pemfaktoran bilangan yang besar menjadi faktor-faktor bilangan prima.

Dengan metode RSA pesan yang akan disampaikan akan diubah menjadi nilai-nilai angka sehingga yang seharusnya 1 karakter akan menjadi beberapa karakter angka sehingga akan memperbanyak jumlah karakter untuk sekali kirim pesan, itulah mengapa peneliti menambahkan metode kompresi (pemampatan) pada penelitian ini.

Kompresi data ialah proses mengubah sekumpulan data menjadi suatu bentuk kode untuk menghemat kebutuhan tempat penyimpanan dan waktu untuk transmisi data. Terdapat banyak metode kompresi, pada penelitian ini metode Shannon-fano yang akan digunakan, berdasarkan kompresi yang dihasilkan metode ini merupakan metode kompresi lossless yaitu metode kompresi data yang menghasilkan data yang sama persis dengan data aslinya dengan merekonstruksi dari data yang dikompres. Berdasarkan tipe peta yang digunakan metode ini merupakan metode statis

dikarenakan menggunakan peta yang sama. Metode ini membutuhkan dua fase, fase pertama menghitung jumlah karakter dan membentuk peta, fase kedua untuk mengubah pesan menjadi kumpulan kode yang akan ditransmisikan.

Berdasarkan latar belakang yang telah disampaikan peneliti akan menguji penggunaan panjang bit kunci yang paling sesuai, tingkat *avalanche effect*, *brute force*, rasio dan *space saving* maka terbentuklah judul penelitian yaitu “IMPLEMENTASI ENKRIPSI DAN KOMPRESI ALGORITMA RSA DAN SHANNON-FANO PADA LAYANAN SMS ANDROID”.

1.2 Rumusan Masalah

SMS masih menjadi pilihan beberapa orang untuk menyampaikan informasi yang penting, namun SMS tidak menyediakan fitur-fitur keamanan seperti yang diterapkan pada *instant messenger (whatsApp, BBM)*, dalam hal ini peneliti ingin membuat aplikasi SMS dengan fitur keamanan, menggunakan algoritma RSA. Algoritma RSA adalah algoritma kunci asimetris dan perhitung matematika bilangan prima, sehingga hasil yang didapatkan dari algoritma ini akan menambah jumlah karakter pesan, sedangkan untuk SMS jumlah karakter terbatas, sehingga perlu dilakukan proses kompresi untuk mengurangi jumlah karakter pesan, algoritma kompresi yang digunakan adalah *Shannon-fano* yang merupakan algoritma *symbolwise*.

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, tujuan dilakukannya penelitian ini adalah sebagai berikut:

1. Menghasilkan aplikasi SMS dengan fitur enkripsi dan kompresi algoritma RSA dan *Shannon-fano*.
2. Mengetahui nilai keamanan dan keefisienan metode RSA dan *Shannon-fano* pada penggunaan SMS.

1.4 Manfaat Penelitian

Hasil penelitian diharapkan dapat mendatangkan manfaat sebagai berikut:

1. Merahasiakan pesan dari orang yang tidak mempunyai hak untuk membaca pesan tersebut.
2. Memperkecil ruang penyimpanan dan mempercepat proses transmisi data.

1.5 Batasan Masalah

Untuk terpusatnya penelitian, maka dibuatkan batasan masalah sebagai berikut:

1. Bahasa pemrograman yang digunakan adalah *Java*.
2. Pesan yang dapat didekripsi adalah pesan yang dikirim dari aplikasi yang dibuat.
3. Panjang kunci maksimal 128 bit.

1.6 Metodologi Penelitian

Untuk melaksanakan penelitian ini ada tahapan-tahapan penelitian dengan rincian sebagai berikut:

1. Survey

Pada tahapan ini dilakukan survey terhadap penelitian apa saja yang sudah diterapkan pada penggunaan layanan SMS, meliputi algoritma sms yang digunakan, algoritma kompresi, dan gabungan dari kedua algoritma tersebut.

2. Studi Literatur

Pembelajaran tentang aplikasi dengan enkripsi dan kompresi yang dikumpulkan dari dokumen, referensi, internet, dan sumber lainnya.

3. Perancangan sistem

Dari pembelajaran literatur dan mengetahui kebutuhan masyarakat terhadap aplikasi yang akan dibuat, maka dilakukanlah analisa terhadap sistem yang akan dibuat, dan dibuatkanlah desain interface untuk aplikasi yang akan dibuat sehingga pada pembuatannya aplikasi siap untuk diimplementasikan.

4. Implementasi

Rancangan dan tampilan yang telah dibuat pada tahapan sebelumnya akan diimplementasikan pada device android dengan menggunakan tools eclipse.

5. Pengujian

Pada tahapan ini akan dilakukan beberapa kali pengujian, dan dari hasil tersebut diketahui seberapa besar tingkat enkripsi dan kompresi.

6. Penyusunan laporan

Tahapan akhir ini dibuatkannya buku laporan untuk pelaksanaan penelitian ini, yang diharapkan dengan adanya buku ini dapat mempermudah untuk pengembangan aplikasi SMS ini menjadi lebih baik.

1.7 Sistematika Penulisan

Laporan tugas akhir ini terdiri dari lima bagian pembahasan, yaitu :

BAB I PENDAHULUAN

Bab ini merupakan bab pembuka yang berisikan latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan penelitian, metodologi penelitian, dan sistematika penulisan untuk penelitian ini.

BAB II STUDI PUSTAKA

Bab ini merupakan bab yang digunakan untuk menjelaskan tentang penelitian yang berisikan tinjauan pustaka yang meliputi penelitian-penelitian sebelumnya yang selaras dengan penelitian, dan landasan teori yang berisikan materi-materi pendukung yang berhubungan langsung dengan penelitian.

BAB III PERANCANGAN SISTEM

Dalam bab ini dijelaskan secara rinci rancangan sistem yang akan digunakan dalam penelitian tugas akhir ini.

BAB IV IMPLEMENTASI SISTEM

Bab ini membahas tentang implementasi sistem yang telah dibuat serta hasil yang diperoleh.

BAB V PENUTUP

Pada bab terakhir ini berisi kesimpulan dari penelitian yang telah dikerjakan. Dan juga saran untuk mengembangkan hasil penelitian ini untuk digunakan dalam penelitian berikutnya.