BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam beberapa tahun terakhir, teknologi pada ponsel telah mengalami perkembangan yang sangat signifikan. Banyak jenis ponsel yang kini bermunculan di pasaran, ponsel yang sebelumnya hanya bisa digunakan untuk sekedar telepon dan sms, sekarang muncul jenis ponsel cerdas yang mempunyai beragam fungsi dan fitur seperti layaknya komputer.

Menurut biro marketing pada laporan kuartal II, Indonesia menduduki peringkat pertama se Asia Tenggara yang warganya terbanyak menggunakan ponsel android. Terdapat 41 juta orang yang menggunakan ponsel android dengan pangsa pasar sebanyak 94%, sedangkan sisanya didominasi oleh iOS dan ponsel lainnya.

Fasilitas ponsel yang masih ramai digunakan hingga kini yaitu layanan pesan singkat (SMS). Dengan fasilitas SMS pengguna dapat melakukan pengiriman pesan singkat dengan begitu mudahnya dalam saling bertukar informasi tanpa batasan jarak dan waktu karena tidak memerlukan koneksi internet.

Pengamanan menjadi aspek penting yang perlu diperhatikan dalam setiap pengiriman dan penerimaan suatu informasi, seperti dalam fasilitas SMS. Namun saat ini, masih terjadinya pembobolan SMS oleh pihak yang tidak bertanggung jawab. Celah keamanan terbesar pada komunikasi melalui SMS terdapat pada mekanisme sistem operator dan pada perangkat ponsel, dimana pesan yang dikirim akan disimpan terlebih dahulu di SMS *Center* dan perangkat ponsel.

Saat ini pun muncul perdebatan mengenai skandal Facebook soal terungkapnya kebocoran data yang berjumlah 50 juta data pengguna yang dikumpulkan oleh *Cambridge Analytica*. Menurut *Cambridge Analytica* yang dimuat oleh merdeka.com menjelaskan selain data pribadi pada akun Facebook pengguna, ternyata Facebook juga mengumpulkan riwayat data SMS pada ponsel android. Hal tersebut telah terjadi selama bertahun-tahun sejak permintaan izin akses di android ke pengguna tak seketat sekarang. Namun tetap saja saat ini pun

Facebook selalu melakukan permintaan izin akses untuk membaca kontak dan pesan. Bahkan Facebook mewajibkan pengguna untuk menggunakan aplikasi Messenger sebagai media perpesanan yang ada pada Facebook. Sehingga ketika ingin membuka pesan masuk Facebook, maka kita akan diwajibkan untuk memasang atau meng-*install* aplikasi Messenger. Dan ketika kita baru menginstal aplikasi Messenger tersebut, maka kita akan dihadapkan dengan tampilan dimana aplikasi akan meminta akses untuk melihat dan memodifikasi kontak maupun SMS. Hal inilah yang menjadikan Facebook dapat mengumpulkan berbagai data telepon maupun SMS dari pengguna android.

Peneliti juga memantau informasi mengenai keamanan pertukaran pesan melalui fasilitas SMS di dalam sebuah grup diskusi, ternyata ada pengguna yang mengeluhkan terjadinya penyampaian pesan yang tidak seharusnya. Pesan SMS yang ia kirim dapat dibaca oleh temannya yang bekerja di operator seluler.

Menurut Kementerian Komunikasi dan Informatika (Kemkominfo), di Indonesia pesan yang disimpan di SMS *Center* adalah format PDU (*Protocol Data Unit*). Format PDU merupakan bentuk heksadesimal oktat dan semi-desimal oktat dari pesan SMS aslinya. Dengan tersimpannya pesan SMS pada SMS *Center*, maka seorang operator seluler yang menangani SMS *Center* dapat dengan mudah memperoleh (membaca) pesan dengan hanya menerjemahkan pesan format PDU, yaitu dengan cara merubah kedalam 8-bit lalu kedalam 7-bit kemudian dirubah ke ASCII. Sedangkan pesan yang tersimpan pada perangkat ponsel merupakan pesan dalam mode teks (pesan asli) sehingga dapat dibaca oleh siapa saja yang mempunyai akses untuk membuka ponsel android.

Dengan fasilitas yang ada, timbul pertanyaan mengenai keamanan pengiriman informasi melalui SMS. Karena itulah dibutuhkan sebuah sistem keamanan dengan menggunakan metode tambahan pada ponsel yang mampu menjaga keamanan isi pesan. Metode yang dimaksud adalah kriptografi, yaitu sebuah seni dan bidang keilmuan dalam penyandian informasi agar tetap aman.

Dalam penelitian ini akan digunakan algoritma kriptografi RSA sebagai metode untuk sistem keamanan tambahan yang akan dibuat. Algoritma RSA dipilih karena dapat memberikan jaminan keamanan lebih dalam melakukan pertukaran

data dibandingkan algoritma lainnya, algoritma RSA membutuhkan 2 buah kunci untuk enkripsi dan dekripsi, dan juga belum ada metode yang dengan formal ditemukan untuk menjebol RSA secara efisien sehingga masih dapat dipercaya dalam protokol-protokol elektronik.

Berdasarkan latar belakang tersebut, maka penulis tertarik memilih judul untuk tugas akhir yakni **"Aplikasi Pengamanan SMS pada Perangkat Android Menggunakan Algoritma Kriptografi RSA"**.

1.2. Identifikasi Masalah

Berdasarkan permasalahan yang telah diuraikan, terdapat permasalahan yang terjadi, yaitu :

1. Pesan yang dikirim melalui fasilitas SMS mempunyai celah keamanan, pesan dapat disadap dan dibaca oleh orang yang memiliki akses ke SMS *Center* dengan menerjemahkan pesan format PDU kedalam 8-bit lalu kedalam 7-bit kemudian dirubah ke ASCII.
2. Pesan yang disimpan dalam perangkat android mempunyai celah keamanan, karena pesan dapat dibuka oleh siapa saja yang mempunyai akses untuk membuka ponsel, sehingga pesan yang tersimpan dapat dibaca.

1.3. Tujuan Penelitian

Tujuan penelitian ini adalah untuk menemukan jawaban berdasarkan identifikasi masalah yang ditemukan. Adapun tujuan penelitian ini, yaitu :

1. Membuat aplikasi android yang dapat menutupi celah keamanan pada pertukaran SMS, dimana pesan akan dienkripsi terlebih dahulu sebelum dikirim dengan menggunakan algoritma kriptografi RSA, sehingga menghasilkan pesan yang aman dikirim dan tidak bisa dibaca begitu saja.
2. Aplikasi yang dibangun akan dilengkapi fitur kode akses masuk agar pesan pada ponsel tidak bocor dan lebih terjaga dari orang yang tidak mempunyai akses masuk.

1.4. Batasan Masalah

Penulis membatasi penelitian yang diteliti, yaitu :

1. Algoritma kriptografi yang digunakan untuk pengamanan pesan adalah algoritma kriptografi RSA.
2. Aplikasi yang dibuat hanya dapat digunakan untuk mengenkripsi teks layanan pesan singkat pada ponsel android.
3. Aplikasi hanya mengamankan isi pesan bukan mengamankan jalur pertukaran pesan.
4. Aplikasi harus dipakai oleh kedua belah pihak, agar pesan enkripsi yang dikirim dapat dibaca oleh si pengirim dan penerima.
5. Aplikasi dapat dijalankan pada android minimal versi *Jellybeans*.
6. Perancangan menggunakan pemrograman Java sebagai bahasa pemrograman dan Android Studio sebagai *editor* pemrograman.

1.5. Manfaat Penelitian

Melalui penelitian ini diharapkan dapat diperoleh manfaat sebagai berikut :

1. Peneliti bisa mengetahui cara mengamankan layanan SMS pada perangkat android.
2. Dapat menerapkan metode kriptografi menjadi aplikasi berbasis android agar dapat digunakan oleh pihak umum.
3. Dapat menjamin keamanan sebuah informasi yang akan dikirim.

1.6. Sistematika Penulisan

Bab I Pendahuluan.

Berisi secara ringkas mengenai latar belakang, identifikasi masalah, tujuan penelitian, batasan masalah, manfaat penelitian, serta sistematika penulisan penelitian.

Bab II Studi Pustaka.

Berisi kajian keislaman yang berkaitan dengan penelitian, konsep teori, konsep pengujian, serta kajian penelitian terdahulu.

Bab III Metodologi Penelitian.

Berisi metode penelitian, tahapan penelitian, kerangka pemikiran, dan waktu penelitian.

Bab IV Analisis dan Perancangan.

Berisi tentang analisis sistem yang meliputi analisis sistem berjalan, analisis permasalahan, analisis solusi, kebutuhan sistem, dan perancangan sistem yang berisi perancangan sistem yang diusulkan.

Bab V Implementasi dan Pengujian

Berisi implementasi dan pengujian bertahap dari program yang dibuat.

Bab VI Kesimpulan

Berisi kesimpulan dari uraian pada bab sebelumnya dan saran untuk pengembangan aplikasi yang dirancang.