Implementasi Keamanan *SMS* Dengan Algoritma RSA Pada *Smartphone* Android

Riad Sahara[1], Hendra Prastiawan[2], Abdul Rohman[3]

[12]Fakultas Ilmu Komputer, Universitas Mercu Buana
[12]Jl. Raya Meruya Selatan, Kembangan, Jakarta Barat 11650
[3]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika
[3]Jl.Daan Mogot KM.13.5 No.9, Cengkareng Jakarta Barat 11730
E-mail: [1]riad.sahara@mercubuana.ac.id, [2]hendra.prastiawan@mercubuana.ac.id

Abstrak

Kebutuhan masyarakat akan adanya pengiriman informasi dari satu tempat ke tempat yang berbeda sudah tidak dapat dipungkiri lagi. Pada zaman sekarang pengiriman informasi telah dipermudah dengan adanya salah satu fitur dari sebuah smartphone, yaitu SMS (Short Message Service), yang mana dapat menggantikan peran surat dalam bertukar pesan. Namun, seiring berjalannya waktu dan berkembangnya zaman, serta perkembangan yang teknologi semakin canggih, muncul beberapa kekurangan pada SMS. Salah satunya yang paling disorot ialah tingkat keamanan SMS tersebut. Tidak dapat dipungkiri bahwa zaman sekarang sudah banyak para pengusaha/petinggi/pejabat pemerintahan yang menggunakan SMS untuk bertukar pesan yang sifatnya sangat rahasia. Sehingga telah banyak terjadi pencurian data SMS atau yang sering disebut penyadapan yang membuat tingkat keamanan SMS perlu ditingkatkan. Untuk mengatasi masalah yang telah diuraikan sebelumnya, peneliti berencana untuk merancang dan membuatkan sebuah aplikasi enkripsi dan dekripsi yang akan diimplementasikan untuk aplikasi SMS pada smartphone android. Aplikasi ini digunakan untuk mengirim dan menerima pesan teks pada smartphone berbasis android dengan mengamankan atau menyembunyikan pesan asli. Sehingga, pengirim tidak perlu takut pesannya akan disadap dan diketahui orang lain yang tidak berkepentingan.

Kata Kunci: Android, Informasi, Kriptografi, Smartphone, SMS.

1. PENDAHULUAN

Kebutuhan masyarakat akan adanya pengiriman informasi dari satu tempat ke tempat yang berbeda sudah tidak dapat dipungkiri lagi. Sejak zaman tradisional pengiriman informasi atau pesan sudah dilakukan dengan menggunakan surat menyurat. Tetapi metode tersebut dirasa banyak memiliki kekurangan salah satunya lamanya waktu yang diperlukan untuk mengirimkan surat tersebut dan sulitnya untuk membuat sebuah surat. Pada zaman sekarang telah dipermudah dengan adanya *SMS* (*Short Message Service*), yang mana dapat menggantikan peran surat dalam bertukar pesan.

Namun, seiring berjalannya waktu dan berkembangnya zaman, serta perkembangan yang teknologi semakin canggih, muncul beberapa kekurangan pada *SMS*. Salah satunya yang paling disorot ialah tingkat keamanan *SMS* tersebut. Tidak dapat dipungkiri bahwa zaman sekarang sudah banyak para pengusaha/petinggi/pejabat pemerintahan yang menggunakan *SMS* untuk bertukar pesan yang sifatnya sangat rahasia. Sehingga telah banyak terjadi pencurian data *SMS* atau yang sering disebut penyadapan yang membuat tingkat keamanan *SMS* perlu ditingkatkan.

Untuk mengatasi masalah yang telah diuraikan sebelumnya, peneliti berencana untuk merancang dan membuatkan sebuah aplikasi enkripsi dan dekripsi yang akan diimplementasikan untuk aplikasi *SMS* pada *smartphone* android. Aplikasi ini digunakan untuk mengirim dan menerima pesan teks pada *smartphone* berbasis android dengan mengamankan atau menyembunyikan pesan asli. Sehingga, pengirim tidak perlu takut pesannya akan disadap dan diketahui orang lain yang tidak berkepentingan.

Berdasarkan latar belakang yang dijelaskan di atas, maka secara garis besar rumusan permasalahan adalah: Bagaimana merancang dan mengimplementasikan suatu aplikasi untuk meningkatkan keamanan *SMS* pada *smartphone* android dengan menggunakan metode *RSA*?

Untuk menghindari pembahasan yang terlalu luas, peneliti akan membatasi masalah yang akan terfokus pada peningkatan keamanan *SMS* pada *smartphone* android dengan mengaplikasikan sistem kriptografi dengan menggunakan metode RSA yang menggunakan bahasa pemrograman Java.

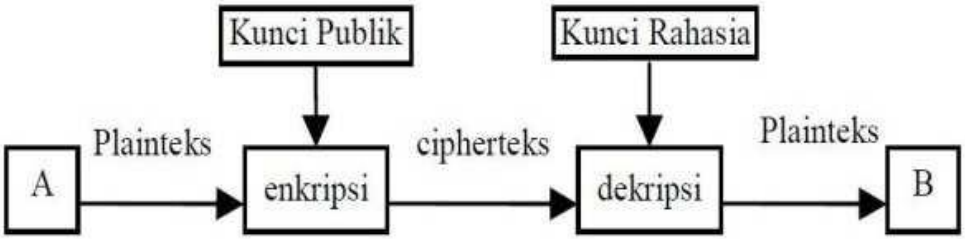
Target inovasi dari penelitian ini yaitu, keamanan dan kenyamanan dalam menggunakan aplikasi SMS pada *smartphone* android untuk berkomunikasi atau mengirimkan informasi.

2. STUDI PUSTAKA

2.1. Algoritma RSA

RSA merupakan algoritma kriptografi asimetris. Ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman. Nama RSA sendiri diambil dari inisial nama depan ketiga penemunya tersebut. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci pribadi. Kunci publik boleh diketahui oleh siapa saja, dan digunakan untuk proses enkripsi. Sedangkan kunci pribadi hanya pihak - pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses dekripsi. Keamanan sandi RSA terletak pada sulitnya memfaktorkan bilangan yang besar. Sampai saat ini RSA masih dipercaya dan digunakan secara luas di internet[5].

RSA adalah metode yang menggunakan perhitungan matematika yang rumit dan disertai dengan kunci pengaman awal (dengan private key maupun dengan public key) sehingga amat sulit untuk ditembus oleh hacker. Adapun prinsip pengamanan metode ini adalah bagaimana sistem dapat mengamankan proses penyimpanan dan pengiriman dokumen. Mula-mula dokumen dalam bentuk teks dienkripsi dengan metode RSA.Sehingga dokumen tidak dapat dibaca oleh siapapun, karena teks telah berubah menjadi susunan huruf yang teracak. Dokumen yang susunan hurufnya telah teracak tersebut jika ingin dibaca oleh pemilik dokumen, maka dokumen tersebut harus dibuka dengan dekripsi RSA kembali.



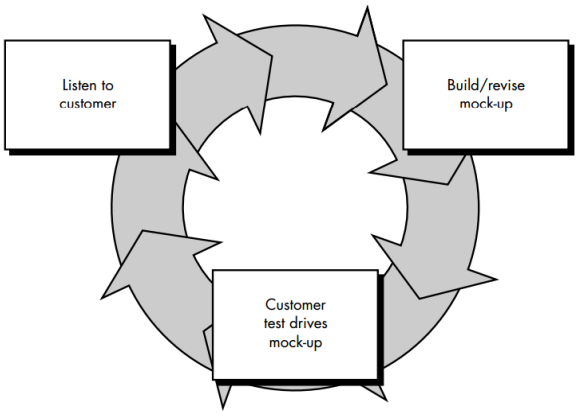
Gambar 1. Skema Kunci Asimetris[10].

3. METODE RISET

3.1. Metodologi Riset

Metodologi pengembangan sistem yang digunakan sebagai tahapan riset adalah *Metode prototyping*. *Prototyping* merupakan salah satu metode pengembangan perangkat lunak atau sistem yang banyak digunakan. Dengan metode ini pengembang dan pelanggan dapat saling berinteraksi selama proses pembuatan sistem. Sering terjadi seorang pelanggan hanya mendefinisikan secara umum apa yang dibutuhkan, pemrosesan dan data-data apa saja yang dibutuhkan. Sebaliknya disisi pengembang kurang memperhatikan efisiensi Algoritma.

Pada *Prototyping* model kadang-kadang klien hanya memberikan beberapa kebutuhan umum software atau sistem tanpa detail *input*, proses atau detail output dilain waktu mungkin tim pembangun (developer) tidak yakin terhadap efisiensi dari algoritma yang digunakan, tingkat adaptasi terhadap sistem operasi atau rancangan *form user interface*. Ketika situasi seperti ini terjadi model prototyping yang sangat membantu proses pengembangan software atau sistem.



Gambar 2. Model *prototype*[7].

3.2. Analisis Masalah

Short Message Service atau yang sering disebut SMS dewasa ini hampir semua perangkat smartphone android menggunakannya. Tetapi dengan semakin berkembangnya teknologi membuat fiture ini memunculkan kekurangan, yaitu tingkat keamanan yang rendah sehingga semakin mudah dicuri pada saat pesan dikirim dari pengirim ke penerima. Sehingga informasi dari fiture tersebut dapat diambil atau disadap oleh orang yang tidak berkepentingan.

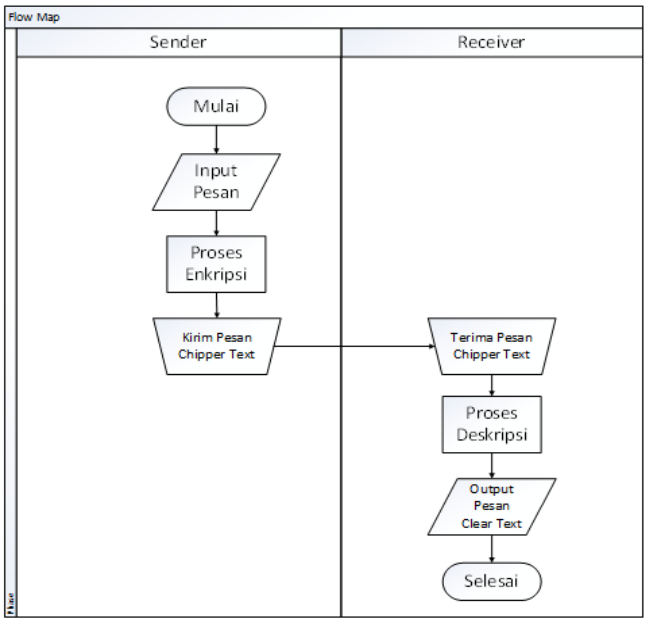
Oleh sebab itu, penggunaan SMS belakangan ini mulai banyak keresahan akan khawatirnya pesan tersebut akan disadap. Khususnya dikalangan pemerintahan atau pengusaha yang memiliki rahasia akan isi dari pesan yang akan dikirim melalui SMS tersebut.

3.3. Solusi Penyelesaian Masalah

Menerapkan kriptografi untuk meningkatkan keamanan dalam bertukar pesan menggunakan SMS dengan metode RSA.

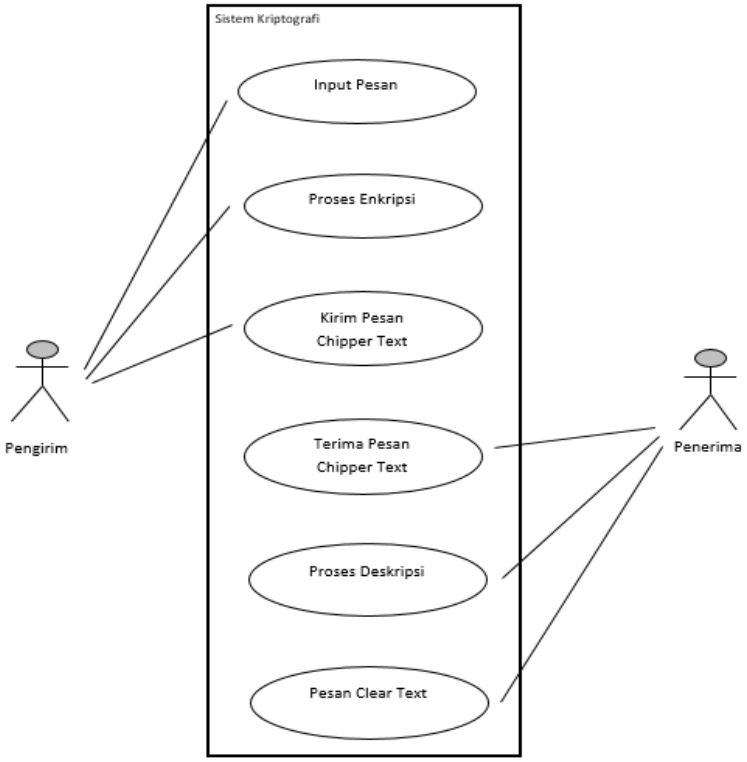
4. PERANCANGAN APLIKASI

4.1. Flow Dokumen (*Flowmap*) Sistem



Gambar 3. Flow Dokumen (*Flowmap*) Sistem

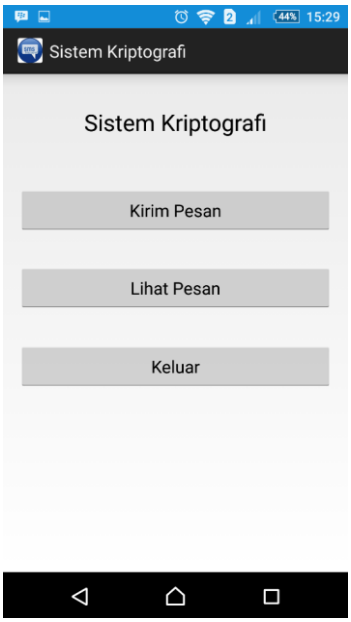
4.2. *Use Case Diagram*



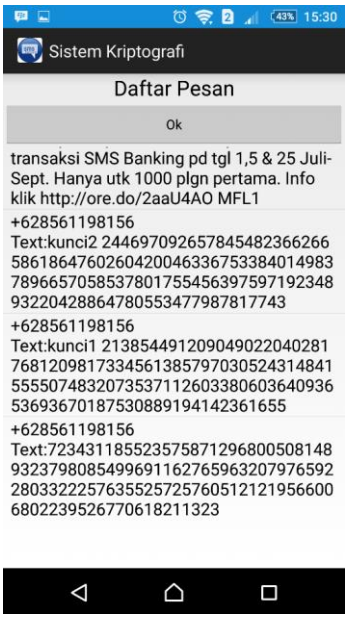
Gambar 4. *Use Case Diagram*

5. IMPLEMENTASI DAN PEMBAHASAN

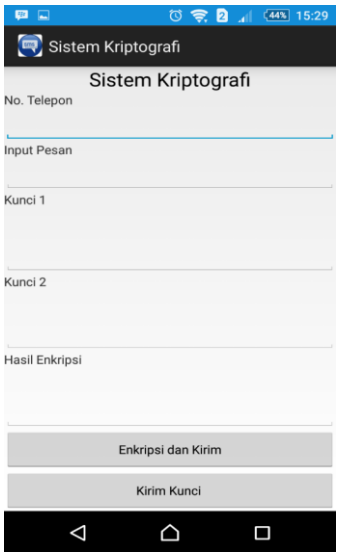
5.1. Implementasi Sistem



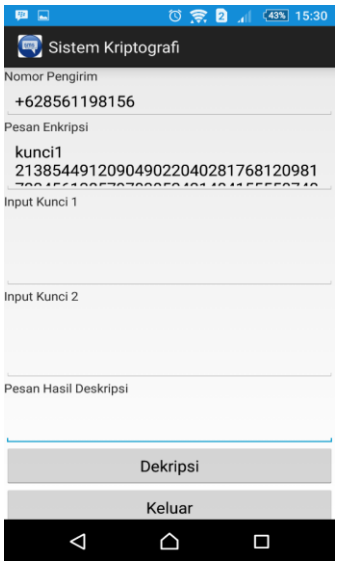
Gambar 5. Tampilan Home



Gambar 7. Tampilan Daftar Pesan



Gambar 6. Tampilan Kirim Pesan (Enkripsi Pesan



Gambar 8. Tampilan Lihat Pesan (Dekripsi Pesan)

5.2. Pengujian Sistem

Tabel 1. Hasil Pengujian Dengan Metode *Black Box*

No	Deskripsi	Kasus Uji	Hasil Pengujian
1	Instal Aplikasi.	Menginstal aplikasi di perangkat Smartphone.	Aplikasi terinstal dengan baik, aplikasi dapat terinstal di smartphone android tanpa hambatan.
2	Menjalankan Aplikasi.	Menjalankan aplikasi.	Aplikasi berjalan dengan baik, tanpa adanya eror.
3	Menu Kirim Pesan	Menginput pesan yang akan dikirim, di enkripsi dan dikirim.	Pesan dapat diinput, dienkripsi dan dikirim dengan baik.
4	Menu Lihat Pesan	Melihat pesan dan mendekripsi pesan.	Pesan dapat didekripsi dan dapat dibaca dengan baik.
5	Menu Keluar	Keluar dari aplikasi	Menu keluar berfungsi dengan baik, aplikasi tertutup setelah di klik menu keluar.

Dari keseluruhan proses pengujian dapat dianalisis bahwa :

1. Aplikasi dapat terinstall dengan baik di smartphone berbasis android.
2. Pada menu Kirim Pesan, Pesan dapat diinput, dienkripsi dan dikirim dengan baik.

3. Pada menu Lihat Pesan, pesan dapat diterima, didekripsi dan dibaca dengan baik.
4. Menu Keluar dapat berfungsi sebagaimana mestinya.

6. PENUTUP

6.1. Kesimpulan

Berdasarkan uraian-uraian yang telah di paparkan pada bab sebelumnya, maka peneliti dapat menarik kesimpulan bahwa pertukaran pesan dengan menggunakan fitur SMS pada zaman modern ini memiliki kelemahan yaitu pada faktor tingkat keamanan pesan, karena pesan dapat disadap oleh orang yang tidak berkepentingan pada saat pesan tersebut dikirim. Dibutuhkannya keamanan tambahan, sehingga peneliti mengimplementasikan enkripsi dan deskripsi pada fitur SMS untuk menguatkan tingkat keamanan pesan. Dengan adanya aplikasi Sistem Kriptografi ini diharapkan dapat mengatasi masalah tersebut.

6.2. Saran

Saran dari penelitian ini adalah mengingat sudah semakin ditinggalkannya fitur SMS pada smartphone, dikarenakan telah terdapatnya fitur yang lebih modern, diharapkan aplikasi ini dapat dikembangkan kembali sehingga dapat digunakan pada aplikasi lain pada smartphone seperti: BBM, whatsapp, path, instagram, telepon, twitter, dll.

7. DAFTAR PUSTAKA

[1] Arifianto, Teguh. (2011). Membuat Interface Aplikasi Android Lebih Keren dengan LWUIT. Yogyakarta: Andi *Publisher*.
[2] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". *Introduction to Modern Cryptography*. p. 10.
[3] Menezes, A. J., van Oorschot, P. C., Vanstone, S. A.Handbook of Applied Cryptography. ISBN 0-8493-8523-7.
[4] Munir, Rinaldi. 2004. Algoritma RSA dan ElGamal. Institut Teknologi Bandung. Departemen Teknik Informatika.
[5] Prayudi, Yudi., Idham Halik. 2005. *Studi Analisis Algoritma Rivest Code 6 (RC6) Dalam Enkripsi/Dekripsi Data*. Seminar Nasional Aplikasi Teknologi Informasi 2005 (SNATI 2005), Yogyakarta.
[6] Riyanto, M. Zaki., & Ardhi Ardian. 2008. *Kriptografi Kunci Publik: Sandi RSA*. http://sandi.math.web.id
[7] Rizal, Ansar, Suharto. 2011. *Implementasi Algoritma RC4 untuk Keamanan Login Pada Sistem Pembayaran Uang Sekolah*. Dielektrika, ISSN 2086-9487 Vol. 2 No.2.
[8] Roger S. Presman, Ph.D.2002. *Rekayasa Perangkat Lunak Pendekatan Praktisi (Buku I).* Andi dan McGraw-Hill Book.
[9] Rosa, A.S., Salahuddin M. 2011. Modul Pembelajaran Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi Objek). Modula, Bandung.
[10] Sadikin, Rifki. 2012. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. Penerbit Andi, Yogyakarta.
[11] Wibowo, Ivan., Budi Susanto., Junius Karel. 2009. *Penerapan Algoritma Kriptografi Asimetris RSA Untuk Keamanan Data Di Oracle.* JURNAL INFORMATIKA, VOLUME 5 NOMOR 1, APRIL 2009.
[12] Wirdasari, Dian. 2008. *Prinsip Kerja Kriptografi dalam Mengamankan Informasi*, Jurnal SAINTIKOM Vol.5 No.2.