

1. Pendahuluan

1.1 Latar Belakang

GPRS merupakan salah satu servis dari GSM yang memungkinkan adanya pertukaran data pada *mobile device* yang telah banyak digunakan di seluruh dunia, salah satu aplikasi yang menggunakan GPRS adalah internet atau intranet. Kenyataannya keamanan pertukaran data pada GPRS merupakan salah satu aspek penting. Apa bila anda seorang anggota badan intelegen atau anggota militer dimana anda mempunyai suatu data atau informasi yang sangat rahasia dan anda berada di daerah yang teletak jauh dari kantor anda, sehingga anda harus mengirimnya, tentunya anda tidak ingin informasi tersebut diketahui pihak umum ataupun pihak-pihak yang tidak kita inginkan. Untuk itu diperlukan suatu mekanisme keamanan untuk menjaga kerahasiaan suatu data. Salah satu mekanisme untuk menjaga keamanan data pada GPRS adalah menggunakan kriptografi dengan algoritma RSA.

RSA merupakan salah satu algoritma kriptografi yang bertipe asimetris yang didasarkan pada kerumitan pempfaktoran pada bilangan bulat yang besar. Algoritma ini terbukti handal dengan tipenya berbentuk asimetri/*public-key cryptosystem* yaitu suatu teknik kriptography menggunakan dua kunci berbeda, kunci yang satu digunakan untuk mengenkrip data menggunakan *public key* dan kunci yang lain digunakan untuk mendekrip data menggunakan *private key*. Hal ini berbeda dengan teknik kriptografi yang bersifat simetri, dimana hanya ada satu kunci untuk mengenkrip atau mendekrip. Dalam hal ini penerima dan pengirim data harus memiliki kunci yang sama. Permasalahan muncul pada saat proses pertukaran kunci antar dua orang. Proses teraman saat pertukaran kunci adalah bertemu secara fisik antar dua orang dan memberikan kunci di tempat yang aman sebelumnya, namun hal ini kurang praktis bila dua orang berada pada jarak yang jauh, bila seandainya dikirim melalui email, maka akan beresiko tercurinya kunci tersebut sehingga membahayakan kewanaman dari kunci tersebut dan berpengaruh pada kewanaman data yang kita kirim. Berbeda dengan teknik asimetri, *public key* tinggal mempublis karena fungsinya hanya untuk men-enkrip data yang dikirim ke pemilik kunci, sedangkan untuk men-dekrip hanya dapat dilakukan oleh pemilik kunci menggunakan *private key*. Didasarkan pada kemampuan algoritma RSA tersebut, diharapkan mampu meningkatkan kewanaman pengiriman data GPRS.

Pada tugas akhir ini akan dibangun suatu sistem keamanan data pada GPRS menggunakan kriptografi dengan algoritma RSA pada *mobile device*. Teknologi yang digunakan untuk membangun aplikasi ini menggunakan J2ME yang notabene merupakan teknologi dari Java yang diperuntukkan dalam pembangunan aplikasi pada *mobile device*.

1.2 Perumusan Masalah

Permasalahan yang menjadi objek penelitian dari tugas akhir ini diantaranya sebagai berikut:

- Bagaimana struktur dan cara kerja dari algoritma RSA.
- Bagaimana membangun suatu keamanan sistem pada GPRS menggunakan kriptografi dengan algoritma RSA pada *mobile device* menggunakan teknologi J2ME.
- Bagaimana performansi waktu pada proses enkripsi dan dekripsi menggunakan algoritma RSA pada *mobile device* menggunakan teknologi J2ME.

1.3 Tujuan Penyusunan

Adapun tujuan yang ingin dicapai dalam penulisan Tugas Akhir ini antara lain:

- Membangun suatu sistem keamanan data pada GPRS menggunakan kriptografi dengan algoritma RSA pada *mobile device* menggunakan teknologi J2ME.
- Menganalisa performansi waktu, yaitu lamanya waktu yang digunakan untuk proses enkripsi dan proses dekripsi pada sistem yang dibangun.

1.4 Batasan Masalah

Dalam penyusunan tugas akhir ini yang menjadi batasan dalam penelitian ini yaitu :

- Algoritma yang analisa pada aplikasi ini hanya RSA, tidak membanding dengan algoritma yang lain, baik berdasar struktur, cara kerja dan efektifitas suatu algoritma terhadap hasil enkripsi pada suatu data. Skema RSA yang dianalisa hanya skema enkripsi, *digital signature* di luar pembahasan tugas akhir ini.
- Data yang di enkripsi pada aplikasi ini berupa data yang berbentuk teks dan gambar (*image*).
- Proses pengiriman kunci publik ke orang lain tidak masuk dalam pembahasan tugas akhir ini.
- Aplikasi yang diterapkan disimulasikan menggunakan emulator *mobile device* khususnya *handphone* yang mendukung J2ME.

1.5 Metodologi Penyusunan

Metodologi penyusunan yang digunakan dalam Tugas Akhir ini , meliputi:

- Studi Literatur :
Mempelajari dasar teori dan literatur-literatur mengenai struktur dan cara kerja algoritma RSA dan penerapannya pada *mobile device* menggunakan J2ME.
- Pengumpulan dan analisa data :
Melakukan pengumpulan informasi dan data-data yang berhubungan dengan pembangunan perangkat lunak.

- Analisa kebutuhan sistem dan perancangan perangkat lunak :
Melakukan analisa kebutuhan perangkat lunak, serta perancangan dan desain perangkat lunak.
- Implementasi dan pengujian perancangan perangkat lunak :
Pengimplementasian terhadap perancangan dan desain yang telah dibuat, kemudian dilakukan pengujian dan analisa performansi dari perangkat lunak yang dibangun.
- Penyusunan laporan :
Laporan yang dihasilkan merupakan buku Tugas Akhir. Penyusunan laporan menggunakan kaidah penulisan laporan yang berlaku.

1.6 Sistematika Penyusunan

Tugas Akhir ini akan disusun berdasarkan sistematika penyusunan sebagai berikut :

BAB I PENDAHULUAN

Menguraikan mengenai latar belakang dari pembahasan Tugas Akhir , perumusan masalah , batasan masalah , tujuan penelitian , metodologi pemecahan masalah , serta sistematika penulisan.

BAB II LANDASAN TEORI

Menguraikan berbagai teori yang berhubungan dengan keamanan pengiriman data menggunakan mobile device, kriptografi, dan yang lain-lain yang berhubungan dengan suatu sistem keamanan data menggunakan kriptografi.

BAB III ANALISA DAN PERANCANGAN PERANGKAT LUNAK

Menguraikan mengenai perancangan serta implementasi dari aplikasi yang akan dibangun.

BAB IV IMPLEMENTASI DAN PENGUJIAN PERANGKAT LUNAK

Menganalisa performansi hasil dari penggunaan algoritma RSA pada sistem yang akan dibangun .

BAB V KESIMPULAN DAN SARAN

Kesimpulan dari keseluruhan rangkaian pengerjaan dan penelitian pada Tugas Akhir yang dilakukan serta saran untuk perbaikan kedepannya.