KEAMANAN DATA PADA GPRS MENGGUNAKAN ALGORITMA RSA BERBASIS J2ME

Krida Kusuma[1], Maman Abdurohman[2], -[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

General Packet Radio Service (GPRS) merupakan salah satu servis pada jaringan Global System for Mobile Communication (GSM). GSM sendiri merupakan teknologi seluler yang saat ini banyak dipakai di seluruh dunia. Dengan GPRS, komunikasi data dapat dilakukan antar mobile device. Salah satu aplikasi yang sudah umum pada GPRS adalah internet atau intranet.

Dalam kenyataannya keamanan data pada GPRS merupakan salah satu aspek penting. Misalkan seorang anggota badan intelegen, tentunya tidak ingin data atau informasinya bocor dan diketahui oleh pihak umum. Untuk itu diperlukan suatu sistem keamanan yang dapat menjaga data pada saat transmisi. Salah satu sistem yang digunakan untuk menjaga kemanan tersebut yaitu kriptografi. Algoritma yang dipakai untuk kriptografi antara lain adalah algoritma Riverst Shamir Adleman (RSA). RSA merupakan salah satu algoritma enkripsi terbukti handal untuk menjaga kerahasiaan suatu data, hal ini dikarenakan RSA merupakan algoritma enkripsi asimetris/public-key cryptosystem , yang memerlukan sepasang kunci, yang satu untuk mengenkrip menggunakan public key dan yang lainnya untuk mendekrip memakai private key. Dalam tugas akhir ini akan dibangun suatu sistem keamanan data pada GPRS menggunakan kriptografi dengan algoritma RSA pada mobile device menggunakan teknologi Java 2 Micro Edition (J2ME). J2ME sendiri merupakan teknologi dari Java untuk membangun sebuah aplikasi pada mobile device.

Kata Kunci : GPRS, GSM, mobile device, kriptografi, RSA, asimetris/public-key

Abstract

General Packet Radio Sevice (GPRS) is one of services on Global System for Mobile Communication (GSM). GSM is celluler communication technology. With GPRS, data communication can did by two or more between mobile device. One of application of GPRS is internet or intranet

The fact of data transmission security on GPRS is a important aspect. Such as a member of Intelegent Insitute or army want to send data that is secret, course he do not want the data is known by public. So that is neened security system to quarantee security while data transmission. One of them is used cryptography. The algorithm that is used for cryptography is Riverst Shamir Adleman (RSA) algoritm. RSA is one of encryption algorithm that security was proofed. It is coused RSA is included to asimtric algorithm or public-key cryptosystem, that has two key, one key for encrypt is called public key and the other for decrypt is called private key.

Keywords : GPRS, GSM, mobile device, cryptography, RSA, asimetric/publickey

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. Kenyataanya 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 pemfaktoran pada bilangan bulat yang besar. Algoritma ini terbukti handal dengan tipenya berbentuk asimetri/*public-key cryptosystem* yaitu suatu teknik kriptograpy 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 kemanan dari kunci tersebut dan berpengaruh pada kemanan 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 kemanan 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 keamananan sistem pada GPRS menggunakan kriptografi dengan algoritma RSA pada *mobile device* menggunakan teknologi J2ME.
- Bagaimana performasi 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 dianalis hanya skema enkripsi, *digital signature* di luar pembahasan tugas akhir ini.
- Data yang di enkripsi pada apliakasi 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 performasi dari perangkat lunak yang dibangun.
- Penyusunan laporan :
  Laporan yang dihasilkan merupakan buku Tugas Akhir. Penyusunan laporan menggunakan kaidah pernulisan 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 kemananan 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.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Beberapa kesimpulan yang dapat diambil adalah sebaga berikut:

1. Waktu untuk proses *generate key*, enkripsi dan dekripsi dipengaruhi oleh besarnya ukuran kunci yang dimasukkan.
2. Semakin besar ukuran kunci yang ditentukan pada proses *generate key*, maka semakin besar pula waktu yang digunakan untuk proses *generate key*.
3. Semakin besar ukuran kunci yang dipakai maka semakin besar pula waktu yang dipakai untuk proses enkripsi dan dekripsi.
4. Besar waktu yang digunakan pada saat dekripsi lebih besar dibandingkan dengan waktu yang digunakan pada proses enkripsi.
5. Pada proses *generate key* dengan ukuran 2048 atau lebih tidak dapat berhasil diproses karena keterbatasan penginisialan tipe data *BigInteger* yang disesuaikan dengan *resource* yang ada pada *mobile device* antara lain memori dan prosesor yang terbatas.
6. Besarnya ukuran kunci yang dipakai menentukan tingkat kerumitan dari hasil proses enkripsi. Semakin besar ukuran kunci yang dipakai maka semakin besar nilai blok *n* yang dipakai dan semakin tinggi tingkat kerumitan yang dihasilkan pada saat proses enkripsi.
7. Ukuran maksimal data yang dapat diproses pada saat enkripsi dan dekripsi dipengaruhi oleh besarnya ukuran kunci yang dipakai.
8. Semakin besar ukuran kunci yang dipakai untuk proses enkripsi dan dekripsi, maka semakin besar pula ukaran maksimal data yang dapat diproses enkripsi dan dekripsi menggunakan ukuran kunci tersebut.
9. Pada ukuran kunci yang sama, ukuran maksimal data yang dapat dienkripsi berbeda dengan saat didekripsi.

5.2 Saran

Berikut beberapa saran untuk pengembangan sistem selanjutnya:

1. Peningkatan ukuran kunci pada *generate key* diharapkan lebih besar untuk meningkatkan tingkat keamanan data.
2. Dalam pengembangan selanjutnya diharapkan ukuran data yang mampu dienkripsi atau didekripsi memiliki ukuran maksimal data yang lebih besar dari sekarang.
3. Sistem tidak hanya dapat untuk enkripsi atau dekripsi teks dan image saja, tapi mampu untuk tipe data yang lainnya.
4. Sistem diharapkan dapat diterapkan pada semua jenis emulator dan *mobile device*.

Daftar Pustaka

[1] Ariyus Doni , “Computer Security”, Semarang : ANDI. 15-11-2005.

[2] B. Knudsen Jonathan, “Java Cryptography”, O’relly, 1998.

[3] Bloch Cynthia, Wagner Annette, “MIDP 2.0 Style Guide for the Java 2 Platform, micro Edition”, Addison Wesley, 10-6-2003.

[4] Cisco IOS mobile wireless Configuration guide “Overview GPRS”, [http://www.cisco.com/univercd/cc/td/doc/product/software/ ios122/122cgcr/fmwire_c/mwcfprt1/mwcfgpov.pdf].

[5] Davis Tom, “RSA Encryption”,[http://www.geometer.org/mathcircles], 10-10-2003.

[6] Grabbe J. Orlin, “Java Program for RSA Encryption”,[http://www.orlingrabbe.com/Java Program for RSA Encryption, by J_ Orlin Grabbe.htm], 2004.

[7] Gupta Vipul, “Securing J2ME[tm] Apllications”, Sun MicroSystems Laboratory, Sun Microsystems, Inc.

[8] J. Yuan Michael “Data Security in Mobile Java Applications”, [http://www.javaworld.com/javaworld/jw-12-2002/jw-1220-wireless_p.html], javaworld, 2002.

[9] Johnston Paul. “Mathematics”, [http://pajhome.org.uk/crypt/rsa/index.html], BSD Lisence, 2004.

[10] R.L. Rivest, A. Shamir, L. Adleman, “A Method for Obtaining Digital Signatures and Public Key Cryptosytems”, Laboratory for Computer Science, Massachusetts Institute of Technology Cambridge.

[11] Raharjo Budi, “Keamanan Sistem Informasi Berbasis Internate”,Bandung:PT. InsanInfonesia, Jakarta:PT. INDOCICS, 2002

[12] “RSA Cryptosystem” , [http://ww3.algorithmdesign.net/handsout/RSA.pdf], 8-6-2002.

[13] Tremblett Paul, "Instant Wireless Java with J2ME",Osborne, 2002.

[14] Wicaksono ady, ”Pemrograman Aplikasi Wireless dengan Java”,Jakarta: PT Alex Media Computindo, 2002.