IMPLEMANTASI ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM UNTUK KEAMANAN SMS

Henry Setyo Ari Bowo[1], Adiwijawa[2], Andrian Rakhmatsyah[3]

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

Abstrak

SMS (Short Messaging Service) merupakan layanan pengiriman pesan dalam lingkungan komunikasi bergerak. Dalam melakukan pengiriman pesan melalui SMS, keamanan pesan merupakan hal yang sangat penting. Pesan yang diamankan bukan hanya pada aspek kerahasiaan, tetapi juga bagaimana pesan tersebut pada saat dikirimkan tidak diubah oleh seseorang sehingga pesan tersebut benar-benar asli. Untuk mengatasi masalah tersebut diperlukan tandatangan digital atau digital signature.

Salah satu cara untuk melakukan digital signature pada pesan yaitu dengan menggunakan fungsi hash. Pembentukan tanda-tangan digital dilakukan dengan menghitung message digest dari pesan dengan menggunakan fungsi hash satu arah. Kemudian mengenkripsi message digest dengan algoritma kriptografi kunci publik. Tanda-tangan digital yang sudah terbentuk diletakkan ke pesan tersebut, lalu keduanya dikirimkan malalui saluran komunikasi. Salah satu algoritma kriptografi kunci-publik yang sering digunakan untuk pembentukan tanda-tangan digital adalah algoritma ECDSA (Elliptic Curve Digital Signature Algorithm). Sedangkan fungsi hash satu-arah yang sering digunakan adalah SHA(Secure Hash Algorithm).

ECDSA sangat cocok untuk dimplementasikan pada SMS yang biasanya melibatkan peralatan mobile device atau hand phone yang memiliki resource yang terbatas. Hal ini dikarenakan ECDSA memiliki kunci yang relatif lebih kecil dibandingkan dengan kriptopgrafi kunci publik yang lain. Dari percobaan yang telah dilakukan dapat ditarik kesimpulan bahwa performansi dari ECDSA pada kasus keamanan SMS ini hanya dipengaruhi oleh panjang kunci yang digunakan, Sedangkan algoritma SHA yang digunakan tidak membarikan pengaruh.

Kata Kunci : SMS, ECDSA, fungsi hash, message digest, digital signature

Abstract

SMS (Short Messaging Service) is messaging delivery service in mobile communications environment. In delivering of message with SMS, messages security is very important. Messages which is saved, not only at the time of messages will be dilivered, but also how messages at the time of delivered are not changed by someone so that messages stills original. To solve this problem needed by digital signature.

One of way to make message digital signature is uses hash function. Digital signature forming is count message digest from message with using oneway hash function. Then message digest is encrypted with public key cryptography algorithm. Digital signature which is formed placed to the message, then both are delivered by communication channel. One of public keycryptography algorithm which is often used for digital signature forming is ECDSA (Elliptic Curve Digital Signature Algorithm) algorithm. While one way hash function which is often used is SHA(Secure Hash Algorithm).

ECDSA is most suitable algorithm to be implentated in SMS which is use mobile device that has limited resource. It is becouse ECDSA relatively has smaller key then other public key cryptography.

From the experiment,ECDSA performance in SMS security is affeceted by the size of the key that used in signing and verifying. SHA algorithm that used in ECDSA is not giving some effect.

Keywords : SMS, ECDSA, hash function, message digest, digital signature

1. Pendahuluan

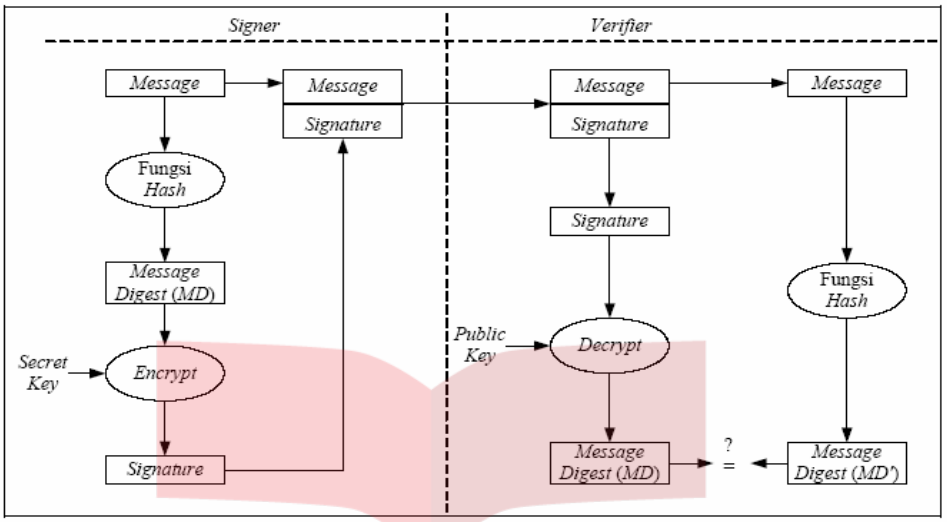
1.1 Latar belakang

Dalam pengiriman pesan melalui SMS (Short Message Service), kemanan pesan SMS yang dikirimkan menjadi sangat penting. Masalah yang sering ada pada keamanan SMS adalah mengidentifikasi pihak yang saling berkomunikasi dan menjaga keaslian pesan yang dikirimkan. Pihak penerima harus dapat memastikan bahwa pesan yang dikirimkan adalah berasal dari pihak pengirim yang dimaksud oleh penerima. Dua pihak yang saling berkomunikasi harus dapat mengautentikasi satu sama lain untuk memastikan pesan dikirim oleh pihak yang benar.

Saat ini SMS banyak digunakan oleh banyak orang sebagai sarana komunikasi. Misalnya seeorang dosen akan memberitahukan tentang jadwal ujian kepada mahasiswanya tentang perubahan jadwal ujian. Mahasiswa tersebut harus dapat memastikan bahwa pesan SMS yang diterimanya adalah benar-benar SMS asli yang berasal dari dosen yang bersangkutan. Bisa saja SMS yang bersangkutan hanyalah berasal dari seseorang yang bermaksud tidak baik terhadap mahasiswa yang bersangkutan. Contoh yang lain adalah SMS banking yang membutuhkan otentikasi pesan yang dikirimkan melalui SMS. Pesan berupa transaksi seperti transfer,update data nasabah,dan sebagainya perlu dibuktikan keaslian dan kebenarannya sebelum transaksi diproses oleh pihak bank. Dengan menggunakan digital signature maka dapat dipastikan valid atau tidaknya pesan yang diterima oleh mahasiswa atau pihak bank tersebut. Hal ini dikarenakan Digital Signature dibangkitkan dari pesan asli yang ditulis olah pengirim. Jika pesan mengalami perubahan maka pesan dianggap tidak valid karena tidak berkorespondensi dengan Digital Signature yang dibuat.

Untuk mengatasi masalah tersebut, pesan yang dikirimkan perlu diberikan tanda tangan digital (Digital Signature). Digital Signature ini dapat dibuat dengan menggunakan fungsi hash satu arah. Pada tugas akhir ini fungsi hash yang digunakan adalah *Secure Hash Algorithm* (SHA). SHA merupakan salah satu fungsi hash yang banyak dianjurkan oleh banyak kriptografer. Hal ini dikarenakan algoritma pendahulunya yaitu MD5 telah ditemukan kolisinya. Kolisi adalah penemuan nilai hash atau message diggest yang sama untuk nilai input yang berbeda. Hal ini dikemukakan oleh Vlastimil Klima pada bulam Maret 2005. Ia berhasil menemukan kolisi pada MD 5 hanya dalam waktu beberapa jam saja menggunakan komputer PC. Oleh karena itu perlu fungsi SHA dinilai lebih baik dari fungsi hash lainnya. Fungsi hash satu arah ini akan menghasilkan message digest yang kemudian akan dienkripsi dengan menggunakan teknik kriptografi kunci publik.

Pada sistem *kriptografi kunci public* atau *asimetrik*, *kunci publik* digunakan untuk proses enkripsi sedangkan kunci privat digunakan untuk proses dekripsi. Akan tetapi dalam pembuatan digital signature ini, *kunci privat* digunakan untuk proses enkripsi sedangkan *kunci publik* digunakan untuk proses dekripsi. Dengan enkripsi menggunakan kunci privat pengirim, autentikasi terhadap pihak pengirim dapat dilakukan. Dengan menggunakan *kriptografi kunci publik* ini, masalah *non repudation* atau penyangkalan dapat diselesaikan. Proses pembuatan dan verifikasi *digital sign*ature dapat dilihat dengan melalui gambar 1.1.



Gambar 1.1 Pembuatan Dan Verifikasi Digital Signature

Salah satu teknik kriptografi kunci publik yang cocok untuk digital signature pada pesan SMS adalah menggunakan kriptografi kurva ellip atau yang sering disebut *Elliptic Curve Criptography* (ECC) yang diperkenalkan oleh Neil Koblitz dan Victor Miller pada tahun 1985. Saat ini kriptografi kurva ellip yang ada saat ini adalah dengan menggunakan pendekatan logaritma diskrit atau sering disebut *Elliptic Curve Diskrit Logaritma Problem* (ECDLP). Hal ini dikarenakan kriptografi kurva ellip ini memiliki panjang kunci yang relatif pendek dibandingkan dengan beberapa kriptografi kunci publik yang lainnya. Salah satu algoritma yang digunakan dalam EDCLP adalah ECDSA (Elliptic Curve Digital Signature Algorithm). Pada tugas akhir ini akan dibahas bagaimana mengimplementasikan ECDSA dalam keamanan pesan SMS.

ECDSA cocok untuk diterapkan pada keamanan pesan SMS karena memiliki panjang kunci yang jauh lebih kecil dari algoritma *kriptografi* lainnya. ECDSA dengan panjang kunci 160 bit memiliki kemampuan yang sama dengan RSA dengan panjang kunci 1024 bit. Dengan panjang kunci yang jauh lebih kecil, maka algoritma ini sangat cocok diimplementasikan pada keamanan pesan SMS yang biasanya melibatkan alat-alat dengan resource terbatas sepeti Handphone atau PDA phone.

Keamanan SMS yang dimaksud dalam tugas akhir ini adalah bagaimana digital signature dapat digunakan untuk mengidentifikasi keaslian pesan dan juga dapat digunakan untuk mengidentifikasi pihal-pihak yang saling berkomunikasi. Pihak pengirim pesan dapat diidentifikasi karena digital signature pada pesan yang akan dikirim dienkripsi dengan menggunakan kunci privat yang hanya dimiliki oleh pihak pengirim. Juga nantinya akan diuji performansi ECDSA jika dimplementasikan untuk keamanan SMS. Performansi yang dimaksud adalah kecepatan aplikasi yang telah dibuat terhadap proses pembuatan *Digital Signature* (*Signing*) dan proses verifikasi *Digital Signature*.

.

1.2 Perumusan masalah

Rumusan masalah pada tugas akhir ini adalah sebagai berikut :

1. Bagaimana mengimplementasikan ECDSA untuk keamanan SMS.
   Keamanan yang dimaksud adalah identifikasi keaslian pesan dan juga autentikasi pihak-pihak yang saling berkomunikasi.

2. Bagaimana performansi algoritma ECDSA jika diimplementasikan pada keamanan SMS.

Maksud dari performansi ini adalah bagaimana kecepatan aplikasi yang telah dibuat terhadap proses pembuatan *Digital Signature* (*Signing*) dan proses *verify Digital Signature*. Selain itu akan dibahas bagaimana pengaruh Digital Signature terhadap panjang pesan SMS.

Sedangkan batasan masalah pada tugas akhir ini adalah

1. Tidak membahas hal-hal yang berhubungan dengan pengiriman atau pentransmisian pesan SMS.
2. Aplkasi dibangun menggunakan bahasa pemrograman Java (J2ME) sehingga hanya dapat digunakan pada Han Phone berbasis GSM.
3. Aplikasi disimulasikan dan diterapkan menggunakan emulator mobile device dan Hand Phone GSM yang mendukukung MIDP 2.0.
4. Algoritma yang digunakan untuk membuat digital signature adalah *Elliptic Curve Digital Signature Algotithm* (ECDSA) dan tidak membahas algoritma kriptografi lainnya.
5. Fungsi *Hash* satu arah yang digunakan adalah SHA

1.3 Tujuan

Tujuan Dari Pembuatan Tugas Akhir ini adalah

1. Menerapkan algoritma ECDSA dalam keamanan SMS.
2. Menguji dan menganalisis peformansi ECDSA.

1.4 Metodologi penyelesaian masalah

Metodologi penyelesaian masalah yang digunakan dalam Tugas Akhir ini adalah sebagai berikut :

1. Studi Literature dan Pendalaman Materi
   Kegiatan-kegiatan yang dilakukan pada tahap Studi Literature dan Pendalaman Materi adalah sebagai berikut :
   1. Mengumpulkan dan memperdalam materi-materi yang berhubungan dengan fungsi *hash* SHA yang digunakan dalam proses pembuatan dan verifikasi *Digital Signature*
   2. Mengumpulkan dan memperdalam materi-materi yang berhubungan dengan Kriptografi Kurva Elliptic yang digunakan untuk proses *enkripsi* dan *dekripsi*.
   3. Mengumpulkan dan memperdalam materi-materi yang berhubungan dengan implementasi ECDSA pada *emulator mobile device*.
2. Analisa dan Perancangan Perangkat Lunak
   Kegiatan-kegiatan yang dilaukan pada tahap analisa dan Perancangan Perangkat Lunak adalah sebagai berikut :
   1. Melakukan analisa terhadap kebutuhan atau *requirement* perangkat lunak yang akan dibangun berdasarkan materi-materi yang telah dikumpulkan sebelumnya.
   2. Membuat desain perangkat lunak berdasarkan analisa yang telah dilakukan sebelumnya.
3. Implementasi dan Pengujian Perangkat Lunak

Kegiatan-kegiatan yang dilakukan pada Implementasi dan Pengujian Perangkat Lunak adalah sebagai berikut :

1. Melakukan Implementasi Perangkat Lunak dengan bantuan bahasa pemrograman yang dapat diterapkan pada *emulator mobile device*.
2. Melakukan Pengujian terhadap Perangkat Lunak yang dibuat.
   Skenario pengujian perangkat lunak adalah sebagai berikut:
   1. Sebelum mengirimkan pesan, perangkat lunak yang ditanamkan pada *emulator mobile device* harus dapat digunakan untuk membuat digital signature.
   2. Setelah pesan dikirimkan dan diterima oleh pihak penerima maka perangkat lunak yang ada pada *emulator mobile device* pengirim harus dapat memverifikasi pesan tersebut asli berasal dari pihak pengirim atau tidak. Jika memang pesan tersebut asli atau sebelum verifikasi dilakukan tidak terjadi perubahan pada pesam, maka perangkat lunak tersebut akan mengeluarkan pesan bahwa pesan valid. Akan tetapi jika sebelum verifikasi *digital signature* pesan diubah terlebih dahulu maka perangkat lunak akan mengeluarkan pesan tidak valid.

4. Analisa Aplikasi yang dibuat.
   Kegiatan-kegiatan yang dilakukan pada tahap ini adalah sebagai berikut :
   1. Melakukan analisa berdasarkan pengujian yang telah dilakukan pada tahap sebelumnya
   2. Membuat kesimpulan berdasarkan analisa yang telah dilakukan sebelumnya.
5. Pembuatan Laporan Tugas Akhir.
   Pembuatan Laporan Tugas Akhir ini adalah pembuatan buku tugas akhir. Laporan ini mencakup semua hal yang berkaitan dengan pembuatan tugas akhir mulai dari pengumpulan materi sampai pembuatan kesimpulan.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Beberapa kesimpulan yang dapat diambil adalah sebagai berikut:

1. Berdasarkan waktu yang digunakan untuk proses signing membutuhkan waktu yang lebih pendek jika dibandingkan dengan proses verifying
2. Berdasarkan penggunaan panjang kunci yang digunakan dapat dilihat bahwa semakin besar panjang kunci yang digunakan maka semakin besar pula waktu yang digunakan untuk melakukan proses signing dan verfying
3. Dilihat dari panjang data yang digunakan sebagai inputan pembuatan digital Signature tidak memberikan pengaruh pada proses signng dan verifying
4. Berdasarkan algoritma SHA yang digunakan ditarik kesimpulan bahwa penggunaan Algoritma SHA yang berbeda tidak memberikan pengaruh pada proses signing dan verfying
5. ECDSA memiliki tingkat keamanan yang cukup tinggi walaupun memiliki ukuran kunci yang relatif lebih pendek jika dibandingkan dengan kunci yang digunakan pada kriptografi kuncipublik lainnya

5.2 Saran

Beberapa saran dalam Tugas Akhir ini adalah sebagai berikut:

1. Algoritma ini bisa diimplementasikan pada kasus yang lain seperti MMS sehingga memungkinkan hasil dan analisa yang berbeda
2. Membandingkan Algoritma ECDSA ini dengan algoritma yang lain sehingga dapat dilihat performansinya dengan algoritma yang lain apakah lebih baik atau lebih buruk

VI Daftar Pustaka

[1] Baselt, Daniel., ”Analysis and Implementation of Offline-Authentication on Mobile Devices”, Heinrich-Heine-Universität Düsseldorf ,Kreklen: 2006

[2] Budiono., “Penerapan Tanda Tangan Digital Untuk Keamanan Transaksi SMS – Banking”, Program Studi Teknik Informatika ITB,Bandung: 2006

[3] Chou, Wendy., “Elliptic Curve Cryptography and Its Applications to Mobile Devices”, Department of Mathematics University of Maryland: 2005.

[4] Ello, Tommy., “A Software Implementation of ECDSA on a Java Smart Card”, Telecommunications Software and Multimedia Laboratory, HELSINKI UNIVERSITY OF TECHNOLOGY: 2006

[5] http://en.wikipedia.org/wiki/ECDSA.htm

[6] http://kur2003.if.itb.ac.id/file/CN-IF5093-Messaging.pdf

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

[8] Kurniawan, Yusuf,. Ir. MT., “Kriptografi Keamanan Internet dan Jaringan Komunikasi”, Penerbit Informatika Bandung: 2006

[9] Munir,Rinaldi., “Kriptografi”, Penerbit Informatika , Bandung: 2006

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

[11] Triwinarko, Andi., “Elliptic Curve Digital Signature Algorithm (ECDSA)”, Program Studi Teknik Informatika ITB, Bandung: 2006.

[12] www.bouncycastle.org