IMPLEMENTASI DIGITAL SIGNATURE ALGORITHM (DSA) DALAM KEAMANAN SMS PADA MOBILE DEVICE

Heri Wibowo[1], Niken Dwi Cahyani[2], Vera Suryani[3]

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

Abstrak

SMS (Short Messaging Service) merupakan layanan pengiriman pesan dalam lingkungan komunikasi bergerak. Selain efektif, SMS tidak memerlukan biaya yang mahal sehingga banyak orang yang menggunakan layanan tersebut. 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 DSA (Digital Signature Algorithm). Sedangkan fungsi hash satu-arah yang sering digunakan adalah SHA(Secure Hash Algorithm).

DSA sangat cocok untuk dimplementasikan pada SMS yang biasanya melibatkan peralatan mobile device atau hand phone yang memiliki resource yang terbatas. Dari percobaan yang telah dilakukan dapat ditarik kesimpulan bahwa performansi dari DSA pada kasus keamanan SMS ini dipengaruhi oleh panjang kunci yang digunakan dan juga algoritma SHA .

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

Abstract

SMS (Short Messaging Service) is messaging delivery service in mobile communications environment. In addition to effective, SMS doesn’t require cost expensive so many people use this service .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 DSA (Digital Signature Algorithm) algorithm. While one way hash function which is often used is SHA(Secure Hash Algorithm).

DSA is most suitable algorithm to be implentated in SMS which is use mobile device that has limited resource. From the experiment, DSA performance in SMS security is affeceted by the size of the key that used in signing and verifying and SHA algorithm

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

1. Pendahuluan

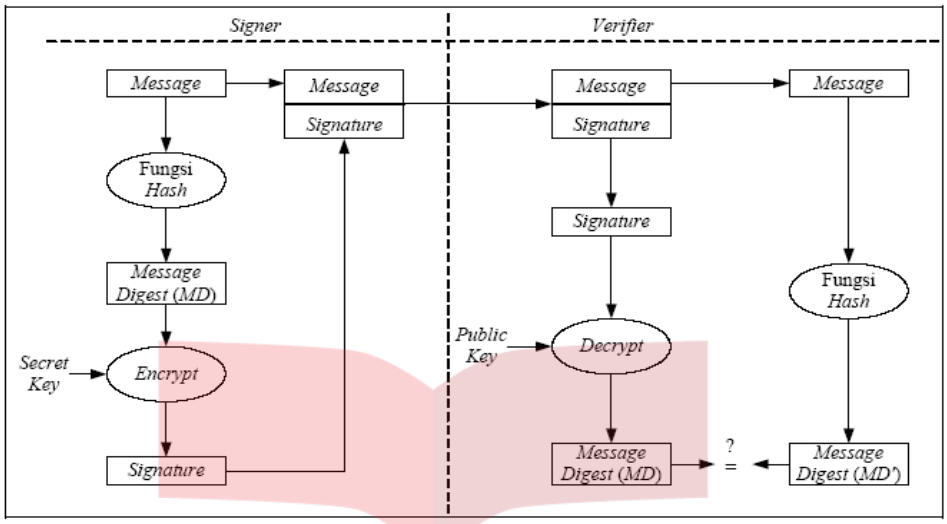
1.1 Latar belakang

SMS (*Short Message Service*) merupakan kebutuhan yang sangat penting saat ini untuk sarana komunikasi. Contohnya ketika seseorang akan memberikan informasi kepada teman yang bertempat tinggal jauh maka dengan adanya fasilitas SMS tersebut informasi dengan cepat dapat diterima. Dengan contoh tersebut sudah dipastikan kalau SMS merupakan suatu fasilitas yang sangat membantu.

Dalam pengiriman pesan melalui SMS, keamanan SMS yang dikirim menjadi sangat penting. Dengan teknologi yang semakin berkembang saat ini, orang menggunakan kepintarannya untuk berbuat baik ataupun jahat. Sehingga dalam mengirim sms harus berhati-hati jika kita menemui orang yang akan berbuat jahat. Dalam hal ini masalah yang sering terjadi pada keamanan SMS yaitu mengidentifikasi pihak yang saling berkomunikasi dan menjaga keaslian pesan yang dikirim apakah pesan tersebut benar-benar dikirim dari orang tersebut atau tidak sehingga pihak penerima harus dapat memastikan kalau pesan yang dikirim memang berasal dari pihak pengirim tersebut. Dua pihak yang saling berkomunikasi harus dapat mengautentikasi satu sama lain untuk memastikan pesan dikirim oleh pihak yang benar. Contoh yang lain misalnya sebuah provider GSM memberikan informasi kepada pelanggannya melalui SMS yang membutuhkan otentikasi pesan. Pesan berupa informasi dari provider tersebut yang perlu dibuktikan keaslian dan kebenarannya. Untuk kasus seperti ini dibutuhkan cara agar dapat memastikan kevalidan pesan yang diterima dari pihak provider maka dibuatlah *digital signature*. Dengan menggunakan *digital signature*, kita dapat memastikan valid atau tidaknya pesan yang diterima. Hal ini dikarenakan *digital signature* dibangkitkan dari pesan asli yang ditulis oleh pengirim. Jika pesan mengalami perubahan maka pesan dianggap tidak valid karena tidak berkorespondensi dengan *digital signature* yang dibuat. Dalam SMS tersebut pesan dengan cepat dapat dikirim ke semua customer.

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 karena 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 publik 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 Gambar1-1 di bawah ini



Gambar 1-1: pembuatan dan verifikasi digital signature

Salah satu metode untuk mengimplementasikan tandatangan digital yang sangat populer dan banyak digunakan adalah metode DSA. Metode ini secara resmi dianjurkan oleh *National Institute of Standards and Technology (*NIST) pada tahun 1991 untuk tandatangan digital yang dinamakan Digital Signature Standard (DSS). Algoritma ini sudah dispesifikasikan oleh badan hukum pemerintah Amerika Serikat yaitu *Federal Information Processing Standard* yang sekarang masih banyak digunakan oleh institut pemerintahan Amerika Serikat.
DSS ini terdiri dari dua komponen :

- Algoritma tandatangan digital yang disebut *Digital Signature Algorithm (DSA)*.
- Fungsi *hash* standard yang disebut *Secure Hash Algorithm (SHA)*

Algoritma DSA merupakan metode untuk penandatanganan pesan dan SHA untuk membangkitkan *message digest* dari pesan. Sebagaimana halnya pada algoritma kriptografi kunci-publik, DSA menggunakan dua buah kunci, yaitu kunci publik dan kunci privat. Pembentukan tanda tangan menggunakan kunci privat, sedangkan verifikasi tanda-tangan menggunakan kunci publik pengirim. DSA menggunakan fungsi *hash SHA* (*Secure Hash Algorithm*) untuk mengubah pesan menjadi *message digest*.

1.2 Perumusan masalah

Rumusan masalah pada tugas akhir ini adalah sebagai berikut :

1. Bagaimana mengimplementasikan DSA untuk keamanan SMS.
   Keamanan yang dimaksud adalah identifikasi keaslian pesan dan juga autentikasi pihak-pihak yang saling berkomunikasi.
   Keamanan DSA dalam kompleksitas secara teori.
2. Bagaimana waktu proses signing dan veryfing dalam algoritma DSA jika diimplementasikan pada SMS.
   Maksudnya adalah faktor apa saja yang mempengaruhi waktu dalam proses pembuatan *Digital Signature* (*Signing*) dan proses verifikasi *Digital Signature*.

Sedangkan batasan masalah pada tugas akhir ini adalah

1. Aplikasi diterapkan pada mobile device.

2. Algoritma yang digunakan untuk membuat digital signature adalah *Digital Signature Algotithm* (DSA) dan tidak membahas algoritma kriptografi lainnya.
3. Fungsi *Hash* satu arah yang digunakan adalah SHA.
4. Tidak membahas hal-hal yang berhubungan dengan pengiriman atau pentransmisian pesan SMS.
5. Aplkasi dibangun menggunakan bahasa pemrograman Java (J2ME) sehingga hanya dapat digunakan pada Hand Phone berbasis GSM.
6. Hand Phone GSM yang mendukung MIDP 2.0.
7. Aplikasi pengirim dan penerima harus hidup (on).

1.3 Tujuan

Tujuan dari pembuatan Tugas Akhir ini adalah

1. Menerapkan algoritma DSA dalam keamanan SMS.
   Untuk mengidentifikasi keaslian pesan dan mengidentifikasi pihak-pihak yang saling berkomunikasi maka digunakan *digital signature* dalam keamanan SMS tersebut. Pihak pengirim pesan dapat diidentifikasi karena digital signature pada pesan yang akan dikirim dienkripsi dengan menggunakan kunci privat yang hanya dimiliki oleh pihak pengirim.
   Keamanan DSA dalam kompleksitas yang dimaksud adalah berapa lama waktu yang dibutuhkan untuk memecahkan algoritma DSA tersebut secara teori
2. Menguji dan menganalisa proses signing dan veryfing dalam DSA jika dimplementasikan pada SMS.
   Apakah proses pembuatan *Digital Signature* (*Signing*) lebih cepat dari pada proses verifikasi *Digital Signature*. Hipotesa sementara yang dapat disimpulkan adalah proses verifikasi akan membutuhkan waktu yang relatif lebih lama dibandingkan dengan proses *signing*.

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 implementasi DSA 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 pesan, 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.
   3. Setelah semuanya selesai, nanti akan di pindahkan ke *mobile device* dan menguji pada *mobile device* langsung
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 dari pada proses verifying
2. Berdasarkan penggunaan panjang kunci yang digunakan bahwa semakin besar panjang kunci yang digunakan maka semakin besar pula waktu yang digunakan untuk melakukan proses signing dan verifying.
3. Dilihat dari panjang data yang digunakan sebagai inputan pembuatan digital signature tidak memberikan pengaruh pada proses signing dan verifying.
4. Berdasarkan algoritma SHA yang digunakan maka disimpulkan bahwa penggunaan SHA1 proses signing dan verifying lebih cepat dari pada SHA 256

5.2 Saran

Beberapa saran agar aplikasi dapat dikembangkan:

1. Sistem dapat dikembangkan lebih lanjut untuk menangani file-file selain file teks
2. Membandingkan metode kriptografi yang lain dalam aplikasi SMS ini sehingga dapat diketahui perbandingan performansi sistem yang satu dengan yang lain
3. Sistem dapat dikembangkan dengan memasukan masalah masalah yang berhubungan dengan pengiriman atau pentransmisian pesan SMS

6. Daftar Pustaka

[1] FIPS PUB 186-3, 2009, Digital Signature Standard (DSS), Nist:

[2] FIPS PUB 180-3, 2008, Secure Hash Standard (SHS), Nist

[3] http://en.wikipedia.org/wiki/DSA.htm

[4] Iswanti Suprapti., "Studi Sistem Keamanan Data dengan Metode Public Key Cryptography", Program Magister Teknik Elektro ITB : 2005

[5] Kurniawan, Yusuf,. Ir. MT., "Kriptografi Keamanan Internet dan Jaringan Komunikasi", Penerbit Informatika Bandung: 2006

[6] Knudsen, Jonathan , "Java Criptography

[7] Munir,Rinaldi., "Kriptografi", Penerbit Informatika , Bandung: 2006

[8] "Pengembangan Aplikasi Sistem Informasi Akademik Berbasis SMS dengan JAVA", Salemba Infotek

[9] Rahayu, Flourensia Sapty, 2005, Cryptography. Fakultas Ilmu Komputer. Universitas Indonesia: Jakarta

[10] Rabah, Kefa , "Security of the Criptographic Protocols Based on Discrete Logarithm Problem", Turkey:Department of Physics, Eastern Mediterrancan University : 2005

[11] Vaudenay, Serge, "The Security of DSA and ECDSA", Swiss Federal Institute of Technologt (EPFL)

[12] www.bouncycastle.org

[13] Weiss, Jason., "Java Cryptography Extensions"