PENERAPAN TANDA TANGAN DIGITAL UNTUK OTENTIKASI SMS - BANKING

Budiono – NIM : 13503013

Program Studi Teknik Informatika, Institut Teknologi Bandung Jl Ganesha 10, Bandung

E-mail : if13013@students.if.itb.ac.id, boedi135@students.itb.ac.id

Abstrak

SMS-Banking merupakan layanan perbankan yang digunakan untuk melakukan transaksi melalui SMS. Layanan ini sangat sering melibatkan nominal yang cukup tinggi. Faktor keamanan menjadi kunci penting dalam keberlangsungan transaksi tersebut. Pada Tugas Akhir ini, telah dikembangkan simulasi sistem *SMS-Banking* yang di dalamnya terdapat penggunaan teknologi tanda-tangan *digital*, sehingga dapat dapat meningkatkan aspek keamanan terutama otentikasi pesan SMS transaksi.

Proses pembentukan dan verifikasi tanda-tangan *digital* dilakukan dengan menggunakan algoritma RSA dan SHA. Panjang kunci yang digunakan oleh aplikasi simulasi yang dijalankan di atas telepon seluler sebesar 256 bit, sedangkan untuk komputer *server* digunakan panjang kunci sebesar 512 bit.

Aplikasi yang dibangun menggunakan teknologi J2SE untuk aplikasi *server* dan J2ME untuk aplikasi *client*. Untuk bilangan *BigInteger* yang digunakan dalam aplikasi *client*, digunakan *source code* yang berasal dari *Bouncy Castle Crypto*.

Berdasarkan hasil pengujian dalam lingkungan *client-server* lokal dan perhitungan waktu pembangkitan sepasang kunci publik dan kunci privat, aplikasi SMS-Banking yang dibangun dengan teknologi tanda-tangan *digital* terbukti mampu meningkatkan keamanan dari segi non teknis, yaitu hanya pihak tertentu saja yang mengetahui kunci privatnya masing-masing.

Kata kunci : *SMS-Banking*, RSA, SHA, tanda-tangan *digital*, *Bouncy Castle Crypto*

1. Pendahuluan

Perkembangan teknologi informasi terutama dalam bidang *mobile* telah membawa perubahan pada masyarakat dalam melakukan komunikasi antar sesamanya. Hal ini dapat dilihat melalui penggunaan sarana pesan singkat atau SMS yang mencapai angka yang cukup tinggi yaitu sekitar 122 juta SMS awal November 2006 (*sumber ww.xl.co.id*). Salah satu contoh penggunaanya adalah untuk sarana transaksi perbankan yang terkenal dengan istilah *SMS-Banking* .

SMS-Banking merupakan suatu layanan bank yang memudahkan nasabah untuk melakukan transaksi perbankan hanya dengan menggunakan perangkat seluler mereka. Transaksi tersebut dilakukan melalui SMS yang dikirimkan secara langsung ke nomor tujuan bank, atau dapat juga terimplementasi dalam SIM *card* telepon seluler nasabah. Aplikasi yang tertanam pada SIM *card* telepon seluler menyimpan beberapa informasi mengenai transaksi yang bisa dilakukan dengan menggunakan tarif SMS. Adapun layanan yang disediakan oleh bank untuk dapat melakukan transaksi melalui SMS, diantaranya ialah cek saldo, cek kurs valuta asing, cek tiga transaksi terakhir, cek tagihan mitra, pembayaran tagihan mitra, pembayaran kartu kredit, dan transfer antar rekening. Layanan *SMS-Banking* menjanjikan mobilitas yang tinggi, bisa dilakukan kapanpun dan dimanapun, bahkan saat *roaming* internasional.

Faktor keamanan menjadi sangat penting semenjak hadirnya produk layanan *SMS-Banking*. Hal ini dikarenakan transaksi perbankan sering melibatkan nilai nominal yang cukup besar sehingga harus memiliki tingkat keamanan yang tinggi. Selama ini sistem keamanan yang ada dilakukan dengan enkripsi pesan SMS yang dilakukan oleh *handphone* dengan menggunakan *key* tertentu yang tertanam pada *SIM card* operator telepon seluler.

Pengguna wajib memasukkan *password* untuk melakukan transaksi tersebut [YUD06].

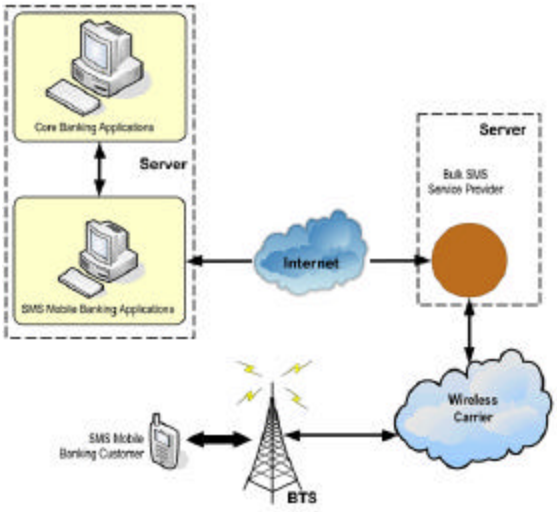
Digital Signature merupakan sebuah teknologi yang dapat digunakan untuk otentikasi pesan elektronik. Teknologi ini mungkin dapat digunakan untuk keamanan dalam transaksi *SMS-Banking*. *Digital signature* dilakukan dengan menggunakan algoritma kunci-publik. Salah satunya adalah algoritma RSA dan dengan menggunakan fungsi *hash Secure Hash Algorithm* (SHA), sehingga proses pembentukan tanda-tangan dari pesan yang dikirim dapat diperiksa keabsahannya. Selain itu penerapan *digital signature* pada SMS dapat meningkatkan keamanan dari aspek non teknis seperti kerahasiaan kunci privat nasabah yang tidak diketahui oleh operator pihak bank[ONN06].

2. Analisis Umum Sistem

Aplikasi *SMS-Banking* ditujukan untuk mengirim data transaksi perbankan ke suatu *server* bank tertentu yang berbasiskan SMS (*Short Message Service*). SMS- Banking merupakan sebuah aplikasi yang menjawab kebutuhan akan pelanggan bank untuk dapat melakukan transaksi perbankan kapanpun dan dimanapun. Untuk itu, bank menyediakan informasi detail mengenai *account* pelanggan dan kemampuan transaksi *real-time* hanya dengan menggunakan perangkat seluler mereka yaitu dengan menggunakan layanan SMS. *SMS-Banking* menyediakan layanan yang dapat digunakan oleh penggunanya secara langsung meliputi :

1. Mendapatkan informasi mengenai saldo pelanggan
2. Mendapatkan informasi mengenai tiga transaksi terakhir
3. Melakukan transfer *account* ke rekenenig pengguna yang lain
4. Membayar tagihan kartu kredit
5. Mendapatkan informasi mengenai kurs valuta asing
6. Melakukan transaksi ubah nomor PIN

Untuk menunjang layanan tersebut, diperlukan sebuah gambaran sistem secara umum mengenai bagaimana proses *SMS-Banking* ini dilakukan dan menghasilkan keluaran yang sesuai dengan keinginan dari bank dan pelanggan. Gambaran mengenai arsitektur *SMS-Banking* terdapat pada Gambar 2-1.



Gambar 2-1 Arsitektur *SMS-Banking* [SAC05]

Dalam melakukan transaksi *SMS-Banking* yang sebenarnya, pelanggan akan mengirimkan sebuah pesan SMS yang berisi sebuah struktur kode tertentu kepada penyedia nomor layanan perbankan tertentu (*Bulk SMS Service Provider*). Nomor layanan yang disediakan oleh *service provider* biasanya berupa nomor pendek yang terdiri dari 4 angka seperti 9386, 8888, 4343, dan sebagainya. Penyedia layanan nomor ini selanjutnya akan meneruskan pesan yang diterimanya ke aplikasi *SMS-Banking* yang ada di bank. Aplikasi *SMS-Banking* yang ada di bank terhubung dengan komputer *server* (*Core Banking Server*) yang menyimpan informasi mengenai rekening bank pelanggan sekaligus melayani permintaan (*request*) dari pelanggan. Hasil permintaan dari pelanggan akan dikirimkan oleh aplikasi *SMS-Banking* ke *Bulk SMS Service Provider* dan dilanjutkan ke nomor telepon seluler pelanggan melalui layanan SMS.

Bank secara proaktif mengirimkan data kepada pelanggan ketika merespon suatu transaksi. Sebagai contoh, transfer *account* dari rekening satu ke rekening yang lain. Data akan dikirimkan ke pelanggan dalam dua metode [SAC05]:

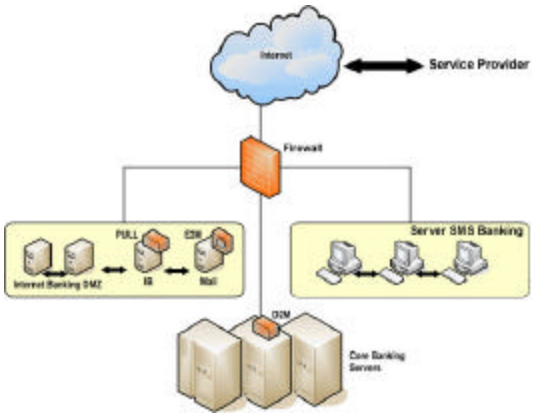
a. *E-mail to mobile* (E2M), bank mengirimkan sebuah email ke aplikasi *SMS-Banking* yang terdapat di bank melalui alamat email yang spesifik. Email ini akan mengandung isi pesan tertentu beserta dengan nomor perangkat seluler pelanggan. Aplikasi *SMS-Banking* yang terdapat di bank mengirimkan pesan dalam format tertentu (sebagai contoh, tag XML yang merupakan bagian dari *string* pesan *query* HTTP GET) ke *server* aplikasi *service provider*. Dari sini, informasi dari tag

XML akan di *extracted* dan dikirimkan sebagai SMS ke nomor telepon seluler pelanggan.

b. *Database to mobile* (D2M), aplikasi *SMS-Banking* yang terdapat di bank akan secara aktif melakukan *polling* ke basis data *server* bank. Sebagai contoh, ketika transaksi pemindahan *account* dari satu rekening ke rekening yang lain, aplikasi mengirimkan pesan tertentu ke aplikasi *server* yang disediakan oleh *service provider*. Format pesan mungkin bisa sama dengan format pada E2M. Pesan ini kemudian dikirimkan sebagai SMS ke nomor telepon seluler pelanggan.

Berdasarkan kedua metode di atas, implementasi tanda-tangan digital SMS untuk *SMS-Banking* akan menggunakan metode D2M. Kelebihan metode ini diantaranya :

1. Proses respon yang diberikan lebih cepat. Hal ini dikarenakan aplikasi langsung berhubungan dengan basis data *server*, tanpa melalui *mail server* terlebih dahulu. Selain itu, protokol komunikasi yang digunakan lebih efektif karena sesuai dengan kebutuhan.
2. Format data yang digunakan lebih dapat disesuaikan dengan kebutuhan tanpa harus melakukan *parsing* lebih seperti pada *parsing* pesan *e-mail*. Parsing *e-mail* dilakukan dengan memisahkan bagian-bagian yang ada seperti *header* (*summary*, *sender*, *receiver*, dan informasi lain) dan *body*(*text*). Padahal yang akan digunakan hanya pada bagian *body* saja. Hal ini mengakibatkan ada proses *parsing* tambahan pada *header* dan *body e-mail* untuk mendapatkan data transaksi. Sedangkan dengan metode D2M, *parsing* dapat langsung dilakukan tanpa harus memisahkan bagian *header* dan *body* karena hanya terdiri dari *body*.
3. Tingkat keamanan dari data yang dipertukarkan lebih aman. Keamanan ini didapatkan karena format data yang dikirimkan hanya diketahui oleh pihak bank. Selain itu proses transaksi yang terjadi hanya terjadi pada jaringan internal bank (LAN). Gambaran mengenai jaringan LAN perbankan untuk *SMS-Banking* terdapat pada Gambar Error! **No text of specified style in document.-2**.



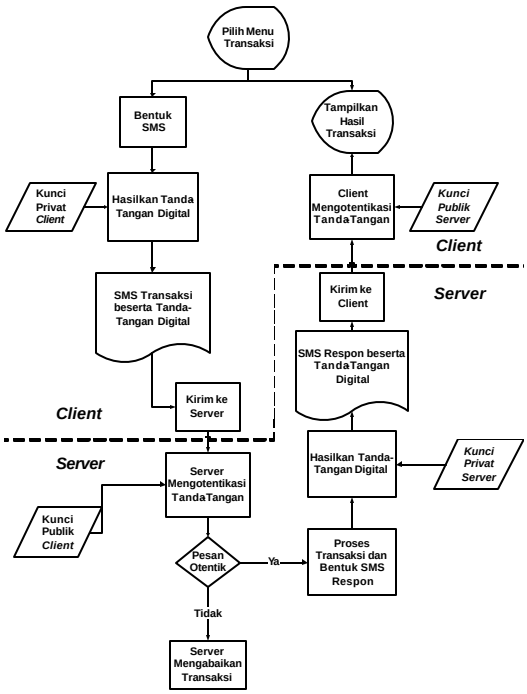
Gambar Error! No text of specified style in document.**-2 Komponen infrastruktur *SMS-Banking* [SAC05]**

Adapun kelemahan dari pemilihan metode D2M ini adalah sebagai berikut :

3. Sistem arsitektur *SMS-Banking* kurang dapat terintegrasi dengan baik dengan fasilitas *e-banking* dari bank yang bersangkutan. Hal ini diakibatkan transaksi melalui *e-banking* kerap menggunakan *e-mail* sebagai protokol komunikasi antara aplikasi server dengan basis data bank.
4. Pengaksesan basis data secara langsung memerlukan otentikasi format *query* yang tepat. Hal ini dimaksudkan agar tidak terjadi kesalahan ketika *entry* sebuah *query*.

3. Analisis Aliran Data *SMS-Banking*

Pada analisis sebelumnya telah dijelaskan mengenai bagan secara umum dan keterhubungan antar komponen yang terdapat pada *SMS-Banking*. Gambar 3- akan menunjukkan diagram alir dari *SMS-Banking*.



Gambar 3-1 Diagram aliran data *SMS-Banking*

Untuk lebih memperjelas bagaimana sebenarnya aliran data yang terjadi dalam *SMS-Banking* akan dijelaskan sebagai berikut :

1. Pelanggan menggunakan aplikasi *SMS-Banking* yang terdapat pada telepon selulernya untuk melakukan transaksi perbankan. Dalam penggunaannya, pelanggan akan memilih menu transaksi perbankan kemudian aplikasi tersebut akan mengubah menu yang dipilih menjadi sebuah bentuk kode tertentu dan mengirimkannya ke dalam bentuk SMS.
2. Sebelum SMS dikirimkan, kode yang terbentuk tersebut akan diberi tanda-tangan *digital* untuk menjamin keamanan pengirimannya ke komputer *server* yang disediakan oleh *service provider* (*Bulk SMS Service Provider*). Pemberian tanda-tangan *digital* ini melibatkan kunci-publik dan kunci rahasia yang digunakan untuk membentuk tanda-tangan *digital.* Untuk beberapa transaksi yang mempunyai isi pesan yang penting, seperti ganti nomor pin, bagian pesan transaksi SMS akan dienkripsi terlebih dahulu dengan menggunakan kriptografi kunci simetri.
3. SMS yang dikirimkan dari perangkat seluler pelanggan akan diterima oleh *Bulk SMS Service Provider* dalam hal ini adalah komputer *server* yang dimiliki oleh penyedia layanan nomor tertentu. SMS yang masuk diterima melalui perangkat GSM *modem* yang terhubung dengan komputer tersebut. SMS yang diterima oleh GSM *modem* tersebut masih mengandung tanda-tangan digital. Komputer lalu akan memeriksa apakah nomor telepon pelanggan dikenali atau tidak. Jika tidak dikenali, maka SMS tidak akan diteruskan pada aplikasi *SMS-Banking* yang terdapat di bank. Setelah dikenali, komputer akan memeriksa apakah format SMS yang diterima telah sesuai dengan format yang ditentukan.
4. Jika SMS memang berasal dari pelanggan yang terdaftar layanan ini dan format SMS telah benar, maka SMS akan diteruskan ke aplikasi *SMS-Banking* yang terdapat di bank. Selanjutnya, aplikasi tersebut akan melakukan verifikasi terhadap data SMS yang diterima untuk memeriksa keabsahannya. Pemeriksaan keabsahan ini berdasarkan tanda-tangan *digital* yang diberikan pada SMS tersebut dengan melibatkan kunci-publik dan kunci privat yang digunakan pada saat pembentukan tanda-tangan *digital*. Kunci yang digunakan pada saat verifikasi merupakan pasangan kunci yang digunakan pada saat pembentukan tanda-tangan digital. Untuk itu, pada komputer ini perlu disimpan tabel pemetaan kunci-publik dari pasangan nilai *e* dan *n*.
5. Jika hasil verifikasi positif, maka disusun *query* untuk transaksi perbankan yang berasal dari pesan SMS tersebut. Setelah itu, *query* akan dikirim ke *server* basis data yang terdapat di bank untuk diproses. Kemudian basis data akan di*update* berdasarkan *query* tersebut.
6. Jika hasil verifikasi negatif, maka data transaksi perbankan yang terdapat pada pesan SMS tersebut diabaikan. Hasil verifikasi negatif ini diakibatkan oleh adanya perubahan pada data SMS sehingga pada saat verifikasi tanda-tangan *digital* yang diperoleh berbeda dengan tanda-tangan *digital* yang diberikan pada awalnya.
7. Hasil verifikasi yang positif akan memicu *server* untuk membentuk SMS hasil *request* dan mengirimkan ke *client* sehingga pengguna dapat melihat dan mengetahui hasi transaksi yang diminta. Setiap SMS yang dikirimkan oleh *server* akan dibubuhkan tanda-tangan *digital* dengan menggunakan kunci publik dari *client*. Proses pertukaran kunci publik dan kunci privat akan dibahas pada subbab selanjutnya.

4. Analisis Keamanan dan Kelayakan Tanda-Tangan *Digital* dengan Fungsi *Hash* dan Algoritma RSA

Pada aplikasi *SMS-Banking*, terdapat penggunaan SMS yang merupakan representasi dari data

transaksi yang digunakan oleh pelanggan dan bank. SMS ini memiliki format tertentu yang telah dibahas pada subbab spesifikasi kebutuhan perangkat lunak sebelumnya. Data sms ini harus tetap terjaga kerahasiaannya (keasliannya) sampai pada saat pemrosesan dan peng-*update*-an basis data bank. Dengan kata lain, data SMS dari pelanggan maupun dari bank harus valid dan teruji keabsahannya.

Data SMS transaksi tersebut dianalogikan sebagai pesan rahasia dimana tidak boleh sembarang orang dapat mengetahuinya. Jaminan keamanan pesan ini tentunya ditangani oleh sistem kriptografi tertentu yang memiliki tingkat kesukaran tinggi. Saat ini sistem kriptografi yang memberikan jaminan keamanan pesan yang tinggi adalah sistem kriptografi kunci-publik dimana kunci rahasia yang digunakan pada sistem kriptografi ini sangat sukar untuk diturunkan dari kunci-publiknya. Sistem kriptografi inilah yang cocok digunakan untuk aplikasi *SMS-Banking*.

Salah satu sistem kriptografi kunci-publik adalah tanda-tangan *digital* dengan algoritma RSA. Tanda-tangan *digital* dengan algoritma RSA sangat tepat digunakan untuk otentikasi data *digital*, seperti pesan yang dikirimkan melalui saluran komunikasi dan dokumen elektronis. Tanda-tangan *digital* tersebut merupakan sistem kriptografi yang tergantung pada isi dokumen dan kunci. Tanda-tangan *digital* RSA direpresentasikan sebagai karakter-karakter heksadesimal dan ditaruh pada akhir SMS. Untuk membedakan tanda-tangan *digital* dengan isi SMS, maka tanda-tangan *digital* RSA diawali dan diakhiri dengan *tag* <s> dan </s>.

Kelayakan penggunaan algoritma RSA untuk tanda-tangan *digital SMS-Banking* dan keamanannya jika dibandingkan dengan DSA, ElGamal atau DES adalah sebagai berikut :

1. RSA sangat cocok digunakan untuk menangani pesan yang berukuran kecil seperti SMS. SMS tergolong sebagai pesan dengan ukuran kecil karena memiliki kapasitas maksimal hanya 160 karakter untuk satu SMS. Sedangkan DSA dan ElGamal lebih tepat untuk menangani pembentukan tanda-tangan *digital* dokumen yang berukuran lebih besar [LEO04].
2. Tingkat keamanan yang diberikan oleh algoritma ini cukup baik. Hal ini dapat dilihat dari tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor primanya, yang dalam hal ini $r = p \times q$. Selain itu, algoritma yang paling mangkus untuk memfaktorkan bilangan yang besar belum ditemukan. Inilah yang membuat algoritma *RSA* tetap digunakan sampai dengan saat ini.
3. Dalam transaksi *SMS-Banking* lebih menekankan kepada otentikasi pesan SMS untuk transaksi selain kepada kerahasiaan pesan. Pihak bank cukup mengetahui bahwa data SMS yang diterimanya merupakan SMS dari pelanggan bank tersebut, begitu juga sebaliknya. Hal ini juga dikarenakan jaringan GSM sudah melakukan enkripsi pesan SMS selama pengiriman pesan dengan menggunakan algoritma kriptografi A5/1 atau A5/2. Dengan kata lain, penggunaan DES untuk menyimpan kerahasiaan pesan kurang signifikan penggunaannya.
4. Dengan menggunakan fungsi *hash*, tanda-tangan *digital* ini dapat menyelesaikan permasalahan *non-repudiation* (baik penerima dan pengirim pesan mempunyai pasangan kunci masing-masing). Penyelesaian tersebut merupakan solusi untuk permasalahan non teknis pada sistem *SMS-Banking* (permasalahan non teknis yaitu dimana operator bank bisa mengetahui kunci yang digunakan pelanggannya).

5. Analisis Protokol Komunikasi Kunci dalam Sistem *SMS-Banking*

Keamanan menjadi faktor yang sangat penting dalam proses transaksi *SMS-Banking*, termasuk pendistribusian kunci publik dan kunci simetri yang akan digunakan oleh pihak pelanggan dan pihak bank. Protokol yang digunakan harus jelas dan aman, sehingga pihak ketiga yang berusaha melakukan penyadapan transaksi tidak dapat melakukannya.

Pendistribusian kunci dalam pembahasan ini merupakan protokol kriptografi yang melibatkan dua belah pihak, yaitu pihak *client* (pelanggan) dan pihak *server* (bank), sedangkan untuk penyedia layanan nomor pendek (*service provider*) tidak termasuk dalam pihak yang terlibat karena fungsinya hanya sebagai perantara transaksi bukan perantara kunci. Pertukaran kunci awal dilakukan ketika pengguna mendaftarkan dirinya ke bank untuk layanan *SMS-Banking*. Untuk pertukaran selanjutnya diserahkan kepada pengguna.

Sebagai ilustrasi, maka pihak pelanggan akan dianggap sebagai *client* dan pihak bank akan dianggap sebagai *server*. Antara *client* dan *server* pada awal penggunaan aplikasi *SMS-Banking* akan saling bertukar kunci publik (pertukaran kunci ini dilakukan di saat pengguna melakukan registrasi layanan *SMS-Banking* ke bank). Kunci publik ini

digunakan terutama dalam proses enkripsi kunci simetri yang dilakukan oleh *client* dan akan dikirimkan ke pihak bank. Transaksi *SMS-Banking* melibatkan kunci simetri untuk melakukan enkripsi terhadap pesan transaksi yang membutuhkan kerahasiaan isi pesannya (nomor seri pesan, ubah PIN, dan transfer uang). Secara lebih jelas, protokol komunikasi yang akan digunakan dalam pembahasan ini terdiri dari 3 bagian, diantaranya :

i. Protokol pertukaran kunci publik

(1) Untuk menggunakan aplikasi *SMS-Banking* pada perangkat seluler, pihak *client* akan diberikan tampilan aplikasi untuk membangkitkan pasangan kunci privat dan kunci publik secara random.
(2) Kunci privat yang dihasilkan akan disimpan dalam perangkat seluler *client*, sedangkan kunci publik akan dikirimkan ke pihak *server* melalui jaringan telepon seluler (GSM).
(3) Ketika pihak *server* telah menerima kunci publik dari *client*, maka saat itu juga, *server* akan membangkitkan sepasang kunci privat dan publik *server*. Kunci privat *server* dan kunci publik *client* yang dihasilkan akan disimpan dalam tabel pemetaan kunci di komputer *server* (**Error! Reference source not found.**). Selanjutnya, kunci publik *server* akan dikirimkan ke *client* melalui jaringan telepon seluler (GSM).

ii. Protokol pertukaran kunci simetri

(1) Setelah menerima kunci public *client*, *server* akan membangkitkan kunci simetri untuk proses enkripsi pesan yang harus tersembunyi informasinya.
(2) Kunci simetri yang dihasilkan akan disimpan dalam aplikasi *server* dan dikirimkan ke pihak *client* bersamaan dengan pengiriman kunci publik. Kunci simetri yang dikirim akan dienkripsikan terlebih dahulu dengan menggunakan kunci publik *client* yang dimiliki oleh *server*.
(3) Pihak *client* akan menerima kunci simetri yang terenkripsi tersebut dan mendekripsikannya dengan menggunakan kunci privat *client* yang dimilikinya. Pihak *server* akan menyimpan kunci simetri yang telah dibangkitkan tersebut dalam tabel pemetaan kunci simetri. Protokol komunikasi transaksi melalui SMS

(1) Untuk setiap pesan perbankan, *client* akan meringkas data SMS menjadi *message digest* dengan fungsi *hash* satu arah.
(2) Pihak *client* mengenkripsi *message digest* dengan kunci privatnya. Hasil enkripsi tersebut akan disertakan sebagai tanda-tangan *digital* pada data transaksi SMS.
(3) Untuk pesan yang mengandung informasi yang penting, maka pada bagian yang rahasia tersebut akan dienkripsi dengan kunci simetri terlebih dahulu lalu dienkripsikan dalam satu kesatuan data transaksi menjadi *message digest* seperti halnya butir diatas.
(4) Pihak *client* mengirim data transaksi SMS yang sudah diberi tanda-tangan *digital* kepada pihak *server*.
(5) Pihak *server* meringkas data transaksi SMS dari *client* menjadi *message digest* dengan fungsi *hash* yang sama. *Server* akan mendekripsikan tanda-tangan *digital* yang disertakan pada data transaksi SMS dengan menggunakan kunci publik *client*. Jika hasil dekripsinya sama dengan *message digest* yang dihasilkan, maka tanda-tangan *digital* tersebut sah.
(6) Protokol ini juga berlaku sebaliknya, antara pihak *server* ke *client*.

6. Pengujian Performansi Algoritma Pembangkitan Kunci

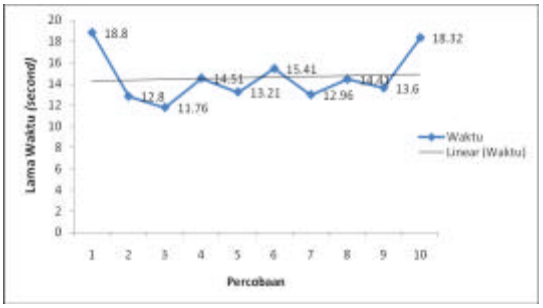
Pengujian performansi algoritma tanda-tangan *digital* dengan RSA untuk membangktikan pasangan kunci publik dan privat diujicoba dengan cara membangkitkan kunci baru pada *client* setiap kali aplikasi *SMS-Banking client* digunakan, dan kemudian menghitung waktu yang dibutuhkan untuk dapat menampilkan tampilan kunci publik dan kunci simetri yang dikirimkan oleh *server*. Tabel hasil uji performansi algoritma pembangkitan sepasang kunci publik dan kunci privat untuk *SMS-Banking* dapat dilihat pada Tabel 6-. Pengujian ini dilakukan pada tanggal 19 November 2007.

Tabel 6-1 Hasil Uji Performansi Pembangkitan Kunci

Percobaan	Pembangkitan kunci client(s)	Pembangkitan kunci server (s)	Waktu client menerima kunci publik server (s)
1	17.95	0.85	80.87

2	12.05	0.75	60.51
3	10.51	1.25	53.59
4	13.36	1.15	62.58
5	12.16	1.05	57.37
6	14.31	1.1	70.33
7	12.06	0.9	67.67
8	13.61	0.8	80.55
9	12.36	1.24	73.55
10	17.27	1.05	57.73

Berdasarkan hasil pengujian yang telah dilakukan, performansi yang dihasilkan untuk pembangkitan pasangan kunci yang digunakan untuk proses pembentukan tanda-tangan digital *SMS-Banking* ini cukup konstan dan hanya berkisar di sekitar 15 detik. Oleh karena itu, dapat disimpulkan bahwa performansi algoritma pembangkitan kunci yang digunakan (RSA dan DES) pada transaksi *SMS-Banking* ini adalah cukup konstan, dan bergantung pada keadaan jaringan GSM. Hal utama yang membuat performansi ini cukup konstan adalah penggunaan panjang kunci 256 bit untuk pembangkitan kunci di *client* dan 512 bit untuk pembangkitan kunci di *server*. Grafik fungsi waktu dan percobaan dari hasil pengujian ini dapat dilihat pada Gambar6-.



Gambar6-1 Grafik Percobaan Pembangkitan Kunci

7. Kesimpulan

Berdasarkan kegiatan-kegiatan yang dilakukan terkait dengan pelaksanaan Tugas Akhir ini, dapat diambil kesimpulan sebagai berikut :

1. Telah berhasil diimplementasikan teknologi tanda-tangan *digital* untuk transaksi *SMS-Banking* yang tersimulasikan dalam perangkat lunak yang telah dibangun. Perangkat lunak tersebut terdiri dari perangkat lunak yang dibangun di atas telepon seluler sebagai *client* dan perangkat lunak yang dibangun di atas komputer sebagai *server*. Keseluruhan perangkat lunak dibangun dengan menggunakan teknologi bahasa pemograman Java.
2. Algoritma RSA dapat diimplementasikan dalam perangkat lunak *client* sebagai komponen yang membentuk tanda-tangan *digital* SMS. Keberhasilan RSA ini terbukti dengan kemampuan perangkat lunak *client* dalam mengoperasikan bilangan *bigintger* sebagai pembangkit pasangan kunci privat dan publik sebesar 256 bit serta tingkat keamanan otentikasi yang telah dibuktikan.
3. Tingkat keamanan otentikasi transaksi *SMS-Banking* dapat ditingkatkan dengan menggunakan model teknologi tanda-tangan *digital* yang diimplementasikan dengan menggunakan algoritma RSA dan SHA. Hal ini dibuktikan dengan keberhasilan penggunaan kunci privat untuk membentuk tanda-tangan digital dan kunci publik untuk memverifikasinya. Tingkat keamanan ini diperkuat dengan digunakannya algoritma DES (kunci simetri) untuk menyembunyikan bagian informasi yang penting seperti nomor seri transaksi, nomor PIN, ataupun nilai transfer transaksi.
4. Penggunaan teknologi tanda-tangan *digital* dapat meningkatkan keamanan dari aspek non teknis. Keamanan tersebut terbukti dengan kerahasiaan kunci privat yang hanya diketahui oleh pengguna aplikasi *client* sehingga pihak bank hanya mengetahui informasi kunci publik pengguna. Hal ini juga berlaku sebaliknya untuk kunci privat yang dimiliki oleh pihak bank.

8. Saran

1. Untuk menguji tingkat keamanan yang lebih baik lagi, dapat dicoba untuk mengimplementasikan teknologi tanda-tangan *digital* dalam sistem perbankan yang *real*.
2. Setiap kali mengirimkan pesan SMS dapat diimplementasikan dengan mengkompresi pesan SMS terlebih dahulu. Kompresi ini ditujukan untuk mengurangi banyaknya karakter yang digunakan dalam membentuk tanda-tangan *digital*. Selain itu juga dapat digunakan pengubahan bentuk tanda-tangan *digital* ke dalam konversi *base64*.
3. Untuk keamanan komunikasi antara *service provider* dengan *server* dapat diimplementasikan dengan algoritma *stream cipher*

[ONN06] Onno W Purbo (2006), Mobile Banking dan Aspek Kemanan, www.trendigital.com/31082003/Artikel/.

[RIV94] R.L. Rivest, A. Shamir, L. Adleman (1994), "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Massachusetts Institute of Technology, Cambridge.

[SAC05] Fauza, M Firda (2006), "Studi dan Perbandingan Keamanan GSM dan CDMA",Institut Teknologi Bandung, Bandung.

[SAC05] Shetty, Sachin. (2005), "SMS Banking", CCNA, BS7799 LA.

[SCH96] Schneir, Bruce. (1996). *Applied Crypthography*. John Wiley.

[BAL06] G. Baldwin Richard (2006), "Digital Signature using Message Digest with Java ", www.developer.com.

[LEI06] Lei Yu (2002), "Generating Digital Signature on Mobile Device", Zhejiang University.

[LEO04] M Leonard Gurning (2004), "Pembangunan Aplikasi Wireless Payment Point Berbasiskan Short Message Service (SMS) : Implementasi Digital Signature dan File Parsing" . Institut Teknologi Bandung, Bandung.

[RIN06] Rinaldi Munir (2006), "Kriptografi" . Institut Teknologi Bandung, Bandung.

[ROM04] R. Romzi Imron (2004), "Membuat Sendiri SMS Gateway Berbasis Protokol SMPP", ANDI, Yogyakarta.