PERANCANGAN DAN IMPLEMENTASI PROTOKOL *SMS-BANKING*

Herdyanto Soeryowardhana – NIM : 13505095

Program Studi Teknik Informatika, Institut Teknologi Bandung Jl. Ganesha 10, Bandung
E-mail : if15095@students.if.itb.ac.id, herdyhsw@gmail.com

Abstrak

SMS atau *Short Message Service* adalah suatu layanan pengiriman pesan singkat melalui telepon seluler. SMS menawarkan banyak kemudahan, salah satunya adalah *SMS-Banking*. *SMS-Banking* merupakan suatu layanan perbankan melalui jalur elektronik yang memungkinkan para nasabah bank tertentu untuk melakukan berbagai transaksi perbankan melalui fasilitas SMS pada telepon seluler.

Pada sistem GSM dan sistem *SMS-Banking* terdapat berbagai ancaman keamanan. Oleh karena itu, pada tugas akhir ini dirancanglah suatu protokol *SMS-Banking* yang dilengkapi dengan berbagai algoritma kriptografi seperti RSA, Rijndael, tanda tangan digital, serta Diffie Hellman. Rancangan protokol tersebut lalu diimplementasikan pada suatu perangkat lunak simulasi yang terdiri dari aplikasi klien dan *server*. Aplikasi klien dikembangkan pada PDA yang berbasis Microsoft Windows Mobile 5.0 sedangkan aplikasi *server* dikembangkan pada komputer yang berbasis Microsoft Windows XP. Kedua aplikasi tersebut dikembangkan dengan menggunakan .NET *framework*.

Tugas akhir ini berfokuskan pada protokol *SMS-Banking*. Metodologi yang digunakan dalam tugas akhir ini yaitu studi literatur, analisis masalah, eksplorasi, analisis perangkat lunak, perancangan perangkat lunak, implementasi perangkat lunak, dan pengujian perangkat lunak. Hasil pengujian pada tugas akhir ini menunjukkan bahwa protokol *SMS-Banking* yang dibuat telah memenuhi tujuan protokol yaitu kerahasiaan, otentikasi, integritas data, serta nirpenyangkalan. Selain itu, protokol telah berhasil diimplementasikan dengan baik pada perangkat lunak simulasi yang dikembangkan. Pengujian penyadapan pesan juga membuktikan bahwa data penting pada pesan yang disadap tidak mudah untuk dikenali.

***Kata kunci**:* protokol*, SMS-Banking,* Windows Mobile *5.0,* .NET *framework*.

1. Pendahuluan

Fasilitas pada telepon genggam yaitu SMS (*Short Message Service*) sudah digunakan oleh masyarakat luas. Menurut data Asosiasi Telepon Seluler Indonesia (ATSI) pada Agustus 2008, jumlah pengguna telepon seluler tercatat sebanyak 120 juta nomor [SIN08]. Telepon seluler pada saat ini sudah menawarkan berbagai fasilitas seperti SMS, percakapan telepon melalui *video* dan *GPRS* (*General packet radio service*) untuk mengakses internet. Di antara fasilitas-fasilitas tersebut, SMS merupakan salah satu fasilitas standard yang didukung oleh telepon seluler termurah saat ini. SMS adalah suatu layanan pengiriman pesan singkat melalui telepon seluler. SMS juga merupakan favorit para pengguna telepon seluler. Hal ini dapat dilihat dari survei yang dilakukan oleh Nielsen Mobile di Amerika pada kuartal kedua tahun 2008 [REA08]. Survei ini menunjukkan bahwa pelanggan telepon seluler di Amerika Serikat lebih banyak menggunakan SMS dibanding melakukan percakapan telepon. Fenomena ini terjadi antara lain karena tarif SMS yang relatif lebih murah dibandingkan tarif percakapan telepon serta terdapat berbagai kemudahan yang ditawarkan oleh SMS, mulai dari pengunduhan nada dering, permintaan berbagai informasi, sampai dengan transaksi perbankan atau *SMS-Banking*.

SMS-Banking merupakan suatu layanan perbankan melalui jalur elektronik yang memungkinkan para nasabah bank tertentu untuk melakukan berbagai transaksi perbankan melalui fasilitas SMS pada telepon seluler. Layanan ini bertujuan untuk memberi kemudahan kepada nasabah dalam memperoleh informasi keuangan

dan melakukan transaksi dimana pun dan kapan pun tanpa harus mengunjungi ATM (Anjungan Tunai Mandiri) atau bank tempat mereka menjadi nasabah [ALM07]. Layanan ini sudah ditawarkan oleh berbagai bank di Indonesia. Fasilitas-fasilitas yang ditawarkan dalam layanan ini hampir sama dengan layanan ATM pada umumnya.

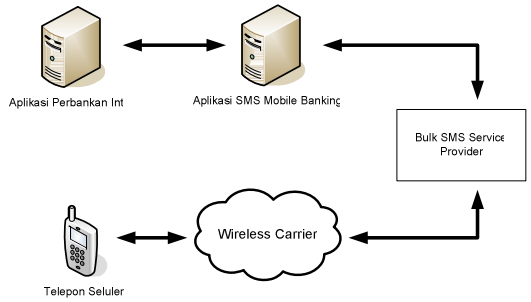
Penggunaan SMS untuk keperluan transaksi perbankan memerlukan perencanaan dan implementasi yang baik. Hal ini dilakukan untuk melindungi para nasabah dari berbagai ancaman keamanan yang muncul dari oknum-oknum yang tidak bertanggung jawab. Saat ini terdapat berbagai ancaman keamanan terhadap sistem *SMS-Banking*. Ancaman yang pertama yaitu *SMS spoofing*. *SMS spoofing* terjadi ketika suatu oknum mengubah informasi identitas pemanggil dirinya menjadi identitas milik orang lain untuk berpura-pura menjadi orang lain pada saat mengirim suatu pesan SMS kepada penerima. Hal itu dilakukan agar penerima mengira bahwa dia menerima pesan SMS dari orang lain [PAN04]. Ancaman kedua yaitu kemungkinan pencurian pesan antara telepon seluler dan *BSS (Base Station Subsystems)*. Ancaman ketiga datang dari personil operator telepon seluler yang dapat dengan mudah membaca isi *log* dari pesan *SMS* yang dikirim oleh pengguna layanan [KOH08]. Ancaman keempat dapat berupa pengiriman pesan kepada *server SMS provider* dengan berpura-pura sebagai aplikasi *mobile banking* [CHI06]. Selain keempat ancaman tersebut terdapat ancaman-ancaman lain yang perlu diwaspadai.

Salah satu cara untuk mengatasi bahaya penipuan yang telah dijelaskan sebelumnya adalah dengan mengimplementasikan suatu protokol *SMS-Banking* yang relatif aman. Secara definitif protokol adalah suatu kumpulan aturan yang mengatur cara suatu pelayanan diberikan [MEH03]. Protokol *SMS-Banking* yang dimaksud di dalam tugas akhir ini mengarah kepada mekanisme pengiriman pesan SMS yang aman antara telepon seluler, *SMS gateway*, dan *server* bank. Protokol ini juga menerapkan berbagai teknologi kriptografi antara lain, algoritma pertukaran kunci seperti Diffie Hellman, algoritma kriptografi simetri seperti AES *(Advanced Encryption Standard)* dan algoritma kriptografi asimetri seperti RSA. Kegunaan algoritma pertukaran kunci adalah untuk mempertukarkan suatu kunci rahasia antara dua orang atau lebih. Algoritma kriptografi asimetri menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi pesan yang berbeda sedangkan pada algoritma kriptografi simetri, kunci yang digunakan adalah sama [MUN09]. Penerapan protokol *SMS-Banking* yang relatif aman diharapkan dapat mengurangi serta melindungi data-data pribadi para nasabah dari berbagai bahaya penipuan dan pencurian oleh oknum-oknum tertentu.

Pada tugas akhir ini digunakan beberapa referensi dari tugas akhir yang telah dibuat sebelumnya. Tugas akhir tersebut adalah tugas akhir yang dibuat oleh Budiono yang berjudul penerapan tanda tangan digital untuk otentikasi *SMS-Banking* [BUD08] dan tugas akhir yang dibuat oleh Rangga Wisnu Adi Permana yang berjudul implementasi algoritma RC6 untuk enkripsi SMS pada telepon seluler [PER08]. Perbedaan antara tugas akhir ini dengan tugas akhir yang lainnya adalah tugas akhir ini lebih menekankan pada aspek perancangan dan implementasi protokol *SMS-Banking* sedangkan pada tugas akhir Budiono lebih menekankan pada penerapan tanda tangan digital dan tugas akhir yang dibuat oleh rangga lebih menekankan pada aspek implementasi algoritma RC6 tersebut.

2. Analisis Sistem *SMS-Banking*

Sistem *SMS-Banking* yang ada pada umumnya memiliki arsitektur sistem seperti yang dapat dilihat pada Gambar 1. Pada awalnya, telepon seluler milik nasabah bank mengirimkan pesan SMS yang berisi kode tertentu kepada nomor penyedia layanan melalui *wireless carrier*. *Wireless carrier* kemudian meneruskan SMS tersebut kepada *Bulk SMS Service Provider*. *Bulk SMS Service Provider* kemudian meneruskan pesan tersebut kepada aplikasi *mobile banking*. Aplikasi *mobile banking* selanjutnya berhubungan dengan *server* perbankan inti untuk memroses permintaan nasabah. Aplikasi *mobile banking* kemudian merespon permintaan nasabah dalam bentuk pesan SMS kepada *Bulk SMS Service Provider*. *Bulk SMS Service Provider* lalu meneruskan SMS tersebut kepada *wireless carrier*. *Wireless Carrier* kemudian meneruskan pesan tersebut kepada telepon seluler nasabah.



Gambar 1 Arsitektur sistem *SMS-Banking* secara umum

Layanan *SMS-Banking* memiliki beberapa pilihan cara yang bisa disesuaikan dengan kemampuan ponsel dan kartu SIM (*Subscriber Interface Module*) yang digunakan, diantaranya:

1. Melalui SMS biasa

Cara ini merupakan cara yang umum digunakan dalam layanan SMS-Banking. Pengguna menggunakan layanan SMS-Banking dengan cara mengetikkan pesan SMS yang berisi kode tertentu yang ditentukan oleh bank, lalu mengirimkan pesan tersebut ke nomor khusus yang sudah ditentukan oleh bank.

2. Melalui menu SIM Toolkit

Pengguna dapat menggunakan layanan SMS-Banking melalui fasilitas yang disediakan oleh operator telepon seluler. Pengguna dapat memilih menu-menu khusus yang dapat diakses pada menu SIM *Toolkit* yakni menu yang biasanya terdapat pada kartu SIM, misalnya: Satelindo@ccess serta M3Access dari Indosat, Life in hand dari ProXL, dan Navigator64 dariTelkomsel.

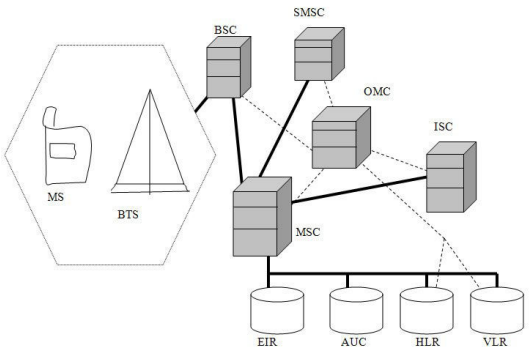
3. Melalui aplikasi khusus.

Pengguna dapat melakukan layanan SMS-Banking melalui aplikasi khusus yang disediakan oleh pihak bank. Aplikasi ini dapat digunakan setelah pengguna terlebih dahulu menanam aplikasi tersebut pada ponselnya. Aplikasi tersebut sangat bergantung kepada spesifikasi ponsel yang dimiliki oleh pengguna sehingga penggunaan dari aplikasi ini cenderung terbatas.

Cara yang pertama yaitu melalui SMS biasa memiliki kelebihan yaitu cara ini tidak bergantung kepada jenis telepon seluler dan memiliki tingkat portabilitas yang sangat baik. Namun, tingkat keamanan dari cara ini tidak terlalu baik karena pesan SMS dikirim dalam bentuk pesan biasa sehingga cukup berbahaya jika pesan tersebut dibaca oleh pihak-pihak yang tidak berkepentingan. Cara yang kedua yaitu melalui menu SIM *Toolkit* memiliki kelebihan dari segi keamanan karena pesan tidak dikirim melalui pesan SMS biasa. Namun, tingkat kebergantungan cara ini cenderung tinggi karena bergantung kepada operator telepon seluler. Cara yang ketiga yaitu melalui aplikasi khusus memiliki kelemahan dalam hal keterbatasan penggunaan karena cenderung bergantung kepada spesifikasi telepon seluler. Namun, cara ini menawarkan tingkat keamanan yang relatif baik jika aplikasi yang dibuat sudah memperhitungkan berbagai aspek keamanan. Oleh karena itu, berdasarkan berbagai kelemahan dan kelebihan dari ketiga cara tersebut, penulis memilih untuk menggunakan cara ketiga yaitu melalui aplikasi khusus dalam tugas akhir ini.

2. Analisis GSM

Arsitektur GSM terdiri atas berbagai macam komponen seperti yang terlihat pada Gambar 2. Garis tebal pada Gambar 2 menunjukkan komunikasi antar komponen inti, sedangkan garis putus-putus menunjukkan koneksi internal untuk komunikasi yang digunakan selama perawatan. Dalam suatu operasi komunikasi biasa, *Mobile Station* (MS) menginisiasi komunikasi tersebut. Sinyal komunikasi ditransmisikan dari MS dan diterima oleh *Base Transceiver Station* (BTS). Fungsi dari BTS antara lain untuk menerima dan mentransmisikan sinyal radio ke dan dari MS, mentranslasikan sinyal radio ke dalam format digital dan mengirimnya kepada *Base Station Controller* (BSC). BSC meneruskan sinyal yang diterima kepada *Mobile Switching Centre* (MSC). MSC menginterogasi *Home Location Register* (HLR) dan *Visitor Location Register* (VLR) yang menyimpan informasi tentang lokasi dari tujuan MS. Jika sinyal yang diterima adalah suatu pesan SMS, maka pesan tersebut akan dirutekan kepada *Short Message Service Centre* (SMSC) untuk pengiriman kepada tujuan yang dibutuhkan. SMSC menyimpan suatu salinan dari SMS yang dikirim ke dalam basis data setelah SMS tersebut terkirim. Dalam suatu kasus koneksi internasional, sinyal kemudian dirutekan melalui *International Switching Centre* (ISC).



Gambar 2 Arsitektur GSM

3. Analisis Protokol *SMS-Banking*

3.1 Tujuan Protokol

Protokol *SMS-Banking* yang dibuat memiliki beberapa tujuan tertentu. Tujuan ini akan menjadi dasar dalam pembuatan protokol *SMS-Banking*. Tujuan dari protokol *SMS-Banking* yang dibuat antara lain:

1. Kerahasiaan

Protokol *SMS-Banking* yang dibuat harus dapat melindungi kerahasiaan data-data yang dimiliki oleh klien dan *server*. Semua data-data yang dimiliki oleh kedua pihak tersebut tidak boleh dibaca atau dimodifikasi oleh pihak-pihak lain yang tidak berkepentingan.

2. Integritas data

Data-data yang terlibat di dalam protokol harus terjaga dari manipulasi oleh pihak-pihak yang tidak berkepentingan. Manipulasi data-data yang dimaksud termasuk penghapusan, pengubahan dan penambahan terhadap data-data yang terlibat di dalam protokol.

3. Otentikasi

Dari sudut pandang klien, protokol harus dapat melakukan otentikasi terhadap *server* sedangkan dari sudut pandang *server*, protokol harus dapat melakukan otentikasi terhadap klien.

4. Non-repudiasi atau nirpenyangkalan

Baik *server* dan klien tidak dapat melakukan penyangkalan terhadap informasi yang tercipta.

3.2 Asumsi Protokol

Asumsi dari protokol ini yang akan dibuat antara lain:

1. Jaringan GSM dianggap ideal dan handal sehingga SMS yang dikirimkan oleh *server* atau klien terjamin sampai pada tujuan.
2. Protokol ini akan menggunakan algoritma kriptografi asimetri sehingga sebelum algoritma ini dapat digunakan, maka dibutuhkan pertukaran kunci publik dan privat antara klien dan *server*. Namun, dalam protokol ini, proses pertukaran kunci publik dan privat milik *server* dan klien tidak termasuk di dalam protokol ini. Pertukaran kunci tersebut dapat dilakukan misalnya melalui email atau melalui ATM. Pada protokol ini, *server* dianggap sudah menyimpan kunci publik milik klien dan kunci privat milik *server* serta klien dianggap sudah menyimpan kunci publik milik *server* dan kunci privat milik klien.
3. Protokol ini memakai kode aktivasi. Kode aktivasi diasumsikan sudah dimiliki oleh klien. Proses klien dalam mendapatkan kode aktivasi tidak termasuk di dalam protokol ini.
4. Arsitektur sistem *SMS-Banking* yang menjadi acuan dalam protokol yang dibuat terdapat pada Gambar III-5. Jaringan antara *Bulk SMS Service Provider* dan *server* bank dianggap sebagai jaringan yang aman dan handal. Dalam arsitektur ini *Bulk SMS Service Provider* hanya bertugas menerima SMS kemudian meneruskan pesan tersebut kepada *server* bank dan mengirimkan SMS kepada tujuan tertentu berdasarkan konfirmasi dari *server* bank.

3.3 Analisis Resiko Keamanan

Terdapat berbagai celah keamanan dalam sistem *SMS-Banking* dan sistem GSM yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Oleh karena itu, dalam subbab ini akan dijelaskan berbagai kemungkinan resiko yang akan muncul.

3.3.1 Kelemahan Algoritma A5

Dalam sistem GSM, algoritma A5 digunakan untuk mengenkripsi data yang ditransmisikan dalam lalu lintas dan saluran persinyalan. Algoritma A5 memiliki dua varian utama yaitu A5/1 dan A5/2. Biyurkov telah menemukan tiga kemungkinan serangan pada versi A5/1 yang biasa digunakan di Eropa. Serangan dapat dilakukan menggunakan suatu komputer personal dalam waktu beberapa detik saja. Varian A5/2 juga dapat diretas dalam waktu kurang dari satu hari. Oleh karena itu, dapat disimpulkan bahwa data yang ditransmisikan pada sistem GSM sudah rawan terhadap serangan kriptanalis.

3.3.2 Kelemahan Algoritma Otentikasi A3 dan A8

Algoritma A3/A8 adalah suatu algoritma otentikasi yang digunakan secara umum di dunia dalam sistem GSM. Meskipun demikian Wagner telah menunjukkan bahwa di telah berhasil mengambil K_i sehingga memungkinkan penggandaan kartu SIM.

3.3.3 SMS Spoofing

SMS spoofing adalah suatu serangan yang melibatkan suatu pihak ketiga yang mengirim pesan SMS yang terlihat seperti dari pihak yang terpercaya. Hal ini terjadi karena dimungkinkan untuk mengganti alamat asli pada *header* SMS dengan suatu *string* alfanumerik pada sistem GSM. Hal tersebut dapat menyembunyikan alamat pengirim dan pengirim dapat mengirimkan pesan palsu.

3.3.4 Masalah Pada Enkripsi SMS

Format data yang umum untuk SMS adalah plainteks. Enkripsi dilakukan pada saat transmisi adalah hanya antara *Base Tranceiver Station* (BTS) dan *Mobile Station*. Namun, seperti yang kita ketahui sebelumnya, algoritma yang digunakan untuk mengenkripsi data yang ditransmisikan antara BTS dan *Mobile Station* yaitu algoritma A5 sudah dapat dipecahkan sistem GSM rawan terhadap pencurian pesan.

3.3.5 Penyalahgunaan Wewenang oleh Personil Pusat SMS

Pada *server* pusat SMS yang dimiliki oleh penyedia layanan jaringan seluler terdapat salinan dari pesan SMS. *Server* pusat yang dimaksud di sini adalah SMSC. Pesan SMS yang disimpan berbentuk pesan berupa teks biasa sehingga setiap personil yang memiliki akses kepada *server* SMS penyedia layanan dapat dengan mudah melihat informasi yang bersifat sensitif secara rinci. Hal ini cukup berbahaya karena terdapat kemungkinan penyalahgunaan terhadap informasi yang dapat dibaca oleh personil yang memiliki akses kepada *server* penyedia layanan.

3.4 Gambaran Umum Protokol

Protokol ini dibuat berdasarkan asumsi dan tujuan yang sudah dijelaskan sebelumnya. Protokol ini terdiri atas dua fase yaitu fase aktivasi dan fase transaksi. Tujuan dari dari fase aktivasi adalah mengaktivasi layanan *SMS-Banking*, membentuk kunci simetri yang akan digunakan pada fase transaksi oleh klien dan *server*, serta mendapatkan nomor urutan yang akan digunakan oleh klien pada fase transaksi. Tujuan dari fase transaksi adalah klien dapat melakukan transaksi perbankan dengan aman serta *server* dapat memroses transaksi yang diminta oleh klien dengan aman dan tepat. Dalam protokol ini, fase aktivasi hanya dilakukan sekali saja ketika klien mengaktivasi *layanan SMS-Banking*, sedangkan fase transaksi dilakukan setiap kali klien ingin melakukan transaksi perbankan Protokol ini menggunakan suatu struktur pesan tertentu untuk memudahkan proses ekstraksi informasi serta proses validasi yang diperlukan

Dalam protokol ini terdapat bagian pesan yang direpresentasikan dalam bentuk *base* 64. Bagian-bagian tersebut antara lain hasil enkripsi, tanda tangan digital, dan nilai Diffie Hellman. Pada awalnya, bagian-bagian tersebut direpresentasikan dalam bentuk *byte*. Namun, agar bagian-bagian tersebut dapat ditampilkan dengan baik pada pesan SMS, maka dilakukan konversi dari *byte* menjadi *base64*.

3.4.1 Fase Aktivasi

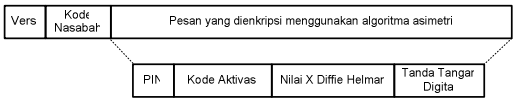
3.4.1.1 Struktur Pesan

Stuktur pesan SMS pada fase aktivasi dibagi menjadi beberapa bagian untuk mengakomodasi berbagai variasi pemeriksaan keamanan yang dibutuhkan dalam protokol. Terdapat dua macam struktur pesan dalam fase aktivasi yaitu struktur pesan fase aktivasi klien dan struktur fase aktivasi *server*. Pada struktur pesan fase aktivasi *server* dan klien terdapat bagian yang dienkripsi menggunakan algoritma asimetri karena pada bagian tersebut terdapat data-data yang tergolong rahasia. Alasan penggunaan algoritma asimetri dalam fase aktivasi ini adalah karena algoritma asimetri dapat digunakan untuk mengamankan pengiriman kunci simetri.

Namun, terdapat juga bagian yang tidak dilakukan enkripsi yaitu pada bagian versi dan kode nasabah. Hal tersebut dimaksudkan agar jika versi protokol pada pesan tidak sesuai dengan versi protokol yang berlaku, maka *server* atau klien dapat segera untuk mengacuhkan pesan tersebut tanpa terlebih dahulu melakukan dekripsi terhadap pesan tersebut sehingga keduanya tidak perlu melakukan komputasi yang sia-sia. Versi terdiri atas kode yang menunjukkan versi dari protokol dan kode yang menunjukkan jenis pesan. Versi memiliki panjang empat digit.

Tiga digit awal merupakan versi protokol sedangan satu digit terakhir merupakan jenis pesan. Selain itu, tidak dilakukan enkripsi pada bagian kode nasabah agar *server* dapat mencari kunci asimetri pada basis data *server* sesuai dengan kode nasabah. Kedua struktur pesan tersebut juga dilengkapi dengan tanda tangan digital menggunakan fungsi *hash* yang digunakan untuk memeriksa keaslian dan isi pesan sehingga berdasarkan tanda tangan digital tersebut dapat diperiksa apakah pesan tersebut telah dimodifikasi atau belum.

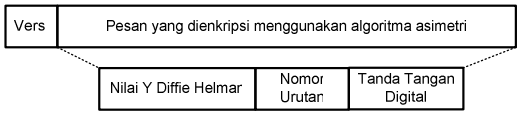
Pada struktur pesan fase aktivasi klien, terdapat PIN yang digunakan untuk proses otentikasi nasabah. Kode aktivasi digunakan untuk menghindari penggunaan pesan secara berulang. Nilai X Diffie Hellman merupakan suatu nilai yang digunakan untuk menghitung kunci simetri berdasarkan pada rumus II-1. Kunci simetri ini akan digunakan pada algoritma kriptografi simetri pada fase transaksi.
Pada struktur pesan fase aktivasi *server* terdapat nomor urutan yang akan digunakan pada fase transaksi. Nomor urutan tersebut digunakan sebagai penanda urutan pesan dan untuk menghindari penggunaan pesan secara berulang pada fase transaksi.



Gambar 3 Struktur pesan fase aktivasi klien

Struktur pesan fase aktivasi klien dapat dilihat pada Gambar 3. Penjelasan untuk struktur fase tersebut adalah sebagai berikut:

1. Versi pada struktur pesan fase aktivasi klien berisi kode 100A.
2. Kode nasabah terdiri atas 10 digit kode khusus nasabah yang bersifat unik.
3. PIN (*Personal Indentification Number*) merupakan nomor rahasia milik nasabah yang memiliki panjang 6 digit.
4. Nilai *X* Diffie Hellman merupakan bilangan yang dihitung berdasarkan suatu nilai yang dipilih klien dengan menggunakan rumus pembangkitan nilai X Diffie Hellman. Nilai X Diffie Hellman memiliki panjang 32 digit.
5. Kode aktivasi merupakan kode khusus yang diberikan oleh pihak bank kepada klien yang digunakan oleh klien untuk mengaktivasi layanan *SMS-Banking*. Kode aktivasi memiliki panjang 6 digit.
6. Tanda tangan digital pada struktur pesan fase *aktivasi* klien merupakan hasil komputasi dari versi, kode nasabah, PIN, kode aktivasi, serta nilai X Diffie Hellman.



Gambar 4 Struktur pesan fase aktivasi *server*

Struktur pesan fase aktivasi *server* dapat dilihat pada 4. Penjelasan untuk struktur fase tersebut adalah sebagai berikut:

1. Versi pada struktur pesan fase aktivasi *server* berisi kode 100B.
2. Nilai *Y* Diffie Hellman merupakan bilangan yang dihitung berdasarkan suatu nilai yang dipilih oleh *server* dengan menggunakan rumus pembangkitan nilai Y Diffie Hellman. Panjang dari nilai ini adalah sebesar 32 digit.
3. Nomor urutan merupakan bilangan yang dibangkitkan oleh *server* yang akan digunakan oleh *server* dan juga klien sebagai penanda urutan pesan pada fase transaksi. Nomor urutan ini memiliki panjang 6 digit.
4. Tanda tangan digital pada struktur pesan fase *aktivasi server* merupakan hasil komputasi dari versi, nilai Y Diffie Hellman, serta nomor urutan.

3.4.1.2 Urutan Protokol

Urutan protokol dalam fase aktivasi adalah sebagai berikut:

1. Klien menghitung tanda tangan digital berdasarkan versi, kode nasabah, nomor urutan, PIN, kode transaksi, isi transaksi I dan isi transaksi II.
2. Klien mengenkripsi nomor urutan, PIN, kode transaksi, isi transaksi I dan isi transaksi II serta tanda tangan digital dengan algoritma simetri menggunakan kunci simetri yang didapatkan dari fase aktivasi.
3. Klien membentuk pesan dengan struktur seperti pada Gambar 3.
4. Klien mengirim pesan SMS kepada *server*.
5. *Server* menerima pesan SMS dari klien.
6. *Server* memeriksa versi protokol.
7. *Server* mendekripsi pesan dengan algoritma simetri menggunakan kunci simetri yang sesuai dengan kode nasabah.
8. *Server* memeriksa kode nasabah, PIN, nomor urutan serta tanda tangan digital pada pesan yang diterima.

9. *Server* memroses transaksi berdasarkan kode transaksi, isi transaksi I dan isi transaksi II. dari pesan.
10. *Server* mengubah nomor urutan menjadi nomor urut yang berikutnya.
11. *Server* menghasilkan tanda tangan digital berdasarkan versi, nomor urutan, dan isi pesan konfirmasi transaksi.
12. *Server* mengenkripsi pesan menggunakan algoritma simetri.
13. *Server* kemudian membentuk struktur pesan SMS seperti pada Gambar 4.
14. *Server* mengirim SMS kepada klien.
15. Klien menerima SMS dari *server.*
16. Klien memeriksa versi protokol.
17. Klien mendekripsi bagian pesan yang diamankan menggunakan algoritma simetri.
18. Klien memeriksa tanda tangan digital.
19. Klien menyimpan nomor urutan yang baru.
20. Klien membaca isi pesan konfirmasi transaksi dari *server*.

3.4.2 Fase Transaksi

3.4.2.1 Struktur Pesan

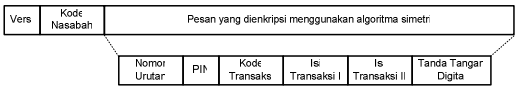
Terdapat dua macam struktur pesan pada fase transaksi yaitu struktur pesan fase transaksi klien dan struktur pesan fase transaksi *server*. struktur pesan fase transaksi klien dapat dilihat pada Gambar III-10 dan struktur pesan fase transaksi *server* dapat dilihat pada Gambar III-11.

Pada kedua struktur pesan tersebut terdapat bagian yang dienkripsi menggunakan algoritma simetri karena pada bagian tersebut terdapat data-data yang tergolong rahasia. Alasan penggunaan algoritma simetri antara lain:

1. Algoritma simetri dirancang sehingga proses enkripsi dan dekripsi pesan membutuhkan waktu yang singkat.
2. Ukuran kunci simetri relatif pendek.
3. Otentikasi pengirim pesan langsung diketahui dari cipherteks yang diterima, karena kunci hanya diketahui oleh pengirim dan penerima pesan saja.

Namun, terdapat juga bagian yang tidak dilakukan enkripsi yaitu pada bagian versi dan kode nasabah. Hal tersebut dimaksudkan agar jika versi protokol pada pesan tidak sesuai dengan versi protokol pada saat itu, maka *server* atau klien dapat segera untuk mengacuhkan pesan tersebut tanpa terlebih dahulu melakukan dekripsi terhadap pesan tersebut. Versi terdiri atas kode yang menunjukkan versi dari protokol dan kode yang menunjukkan jenis pesan. Versi memiliki panjang empat digit. Tiga digit awal merupakan versi protokol sedangan satu digit terakhir merupakan jenis pesan. Kedua struktur pesan tersebut juga dilengkapi dengan tanda tangan digital menggunakan fungsi *hash* yang digunakan untuk memeriksa keaslian dan isi pesan sehingga berdasarkan tanda tangan digital tersebut dapat diperiksa apakah pesan tersebut telah dimodifikasi atau belum. Selain itu, tidak dilakukan enkripsi pada bagian kode nasabah agar *server* dapat mencari kunci simetri pada basis data *server* sesuai dengan kode nasabah.

Pada struktur pesan juga terdapat PIN yang digunakan untuk proses otentikasi nasabah. Nomor urutan yang didapatkan dari fase aktivasi dipakai oleh klien pada fase transaksi ini. Nomor urutan akan diubah menjadi urutan berikutnya ketika *server* telah menyelesaikan proses transaksi yang dimiliki oleh klien.
Pada struktur pesan pada fase transaksi terdapat kode transaksi, isi transaksi I, dan isi transaksi II. Kode transaksi merupakan kode khusus yang mengacu kepada suatu layanan transaksi sedangkan isi transaksi I dan isi transaksi II berisi data-data yang diperlukan oleh layanan transaksi yang terkait. Contohnya, isi dari kode transaksi adalah 101 yang mengacu kepada layanan transfer antar rekening, maka isi dari isi transaksi I adalah nomor rekening tujuan dan isi dari isi transaksi II adalah nominal jumlah uang yang akan ditransfer.



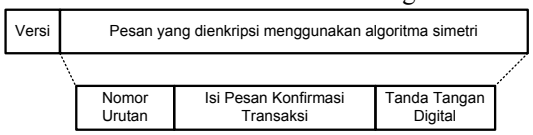
Gambar 5 Struktur pesan fase transaksi klien

Struktur pesan fase transaksi klien dapat dilihat pada Gambar 5. Penjelasan untuk struktur fase tersebut adalah sebagai berikut:

1. Versi pada struktur pesan fase transaksi klien berisi kode 100C.
2. Kode nasabah terdiri atas 10 digit kode khusus nasabah yang bersifat unik.
3. PIN (*Personal Indentification Number*) merupakan nomor rahasia milik nasabah yang memiliki panjang 6 digit.
4. Kode transaksi merupakan kode khusus yang sudah ditentukan berdasarkan layanan transaksi yang diinginkan oleh nasabah. Kode ini memiliki panjang 3 digit.
5. Isi transaksi I dan isi transaksi II adalah data-data yang berkaitan dengan kode transaksi yang diminta yang masing-masing memiliki panjang 10 digit.
6. Tanda tangan digital yang dihasilkan pada pesan permintaan transaksi dari klien dihitung berdasarkan versi, kode nasabah,

nomor urutan, PIN, kode transaksi, isi transaksi I, dan isi transaksi II.

7. Nomor urutan merupakan nomor urutan yang didapatkan dari fase *aktivasi*. Panjang nomor urutan adalah sebesar 6 digit.



Gambar 6 Struktur pesan fase transaksi *server*

Penjelasan dari bagian-bagian dari struktur pesan di atas dijelaskan sebagai berikut:

1. Versi pada struktur pesan fase transaksi *server* berisi kode 100D.
2. Isi pesan konfirmasi berisi pesan konfirmasi dari layanan transaksi perbankan yang berhasil diproses oleh *server* bank.
3. Nomor urutan merupakan nomor urutan baru yang didapatkan dari *server*. Panjang nomor urutan adalah sebesar 6 digit.

3.4.2.2 Urutan Protokol

Urutan protokol dalam fase transaksi adalah sebagai berikut:

1. Klien menghitung tanda tangan digital berdasarkan versi, kode nasabah, nomor urutan, PIN, kode transaksi, isi transaksi I dan isi transaksi II.
2. Klien mengenkripsi nomor urutan, PIN, kode transaksi, isi transaksi I dan isi transaksi II serta tanda tangan digital dengan algoritma simetri menggunakan kunci simetri yang didapatkan dari fase transaksi.
3. Klien membentuk pesan dengan struktur seperti pada Gambar 5.
4. Klien mengirim pesan SMS kepada *server*.
5. *Server* menerima pesan SMS dari klien.
6. *Server* memeriksa versi protokol.
7. *Server* mendekripsi pesan dengan algoritma simetri menggunakan kunci simetri yang sesuai dengan kode nasabah.
8. *Server* memeriksa kode nasabah, PIN, nomor urutan serta tanda tangan digital pada pesan yang diterima.
9. *Server* memroses transaksi berdasarkan kode transaksi, isi transaksi I dan isi transaksi II. dari pesan.
10. *Server* mengubah nomor urutan menjadi nomor urut yang berikutnya.
11. *Server* menghasilkan tanda tangan digital berdasarkan versi, nomor urutan, dan isi pesan konfirmasi transaksi.
12. *Server* mengenkripsi pesan menggunakan algoritma simetri.
13. *Server* kemudian membentuk struktur pesan SMS seperti pada Gambar 6.
14. *Server* mengirim SMS kepada klien.
15. Klien menerima SMS dari *server.*
16. Klien memeriksa versi protokol.
17. Klien mendekripsi bagian pesan yang diamankan menggunakan algoritma simetri.
18. Klien memeriksa tanda tangan digital.
19. Klien menyimpan nomor urutan yang baru.
20. Klien membaca isi pesan konfirmasi transaksi dari *server*.

4. Deskripsi Umum Perangkat Lunak

Perangkat lunak yang dibangun merupakan suatu simulasi *SMS-Banking* berdasarkan protokol *SMS-Banking* yang sudah dirancang sebelumnya. Seluruh tahapan pada fase aktivasi dan fase transaksi pada protokol *SMS-Banking* yang harus dapat dijalankan pada perangkat lunak ini. Nama perangkat lunak tersebut adalah HIPRO SMS.

Secara umum HIPRO SMS terdiri atas dua bagian utama yaitu klien dan server. Bagian klien merupakan aplikasi yang berjalan di atas telepon seluler pengguna. Tugas dari bagian ini adalah menjalankan protokol baik untuk fase aktivasi maupun fase transaksi pada bagian klien serta menyediakan antarmuka yang dibutuhkan oleh nasabah untuk melakukan aktivasi layanan perbankan serta melakukan layanan transaksi perbankan. Aplikasi yang dibangun pada bagian *server* bertugas menjalankan protokol baik untuk fase aktivasi maupun fase transaksi pada bagian *server*. Proses otentikasi pesan SMS dan pemrosesan transaksi *SMS-Banking* dilakukan pada bagian ini.

5. Pengujian

5.3 Tujuan Pengujian

Tujuan dari pengujian yang dilakukan antara lain:

1. Menguji kesesuaian protokol *SMS-Banking* yang dibuat dengan tujuan protokol.
2. Mengetahui apakah protokol *SMS-Banking* yang dibuat dapat diimplementasikan dengan baik pada perangkat lunak simulasi.
3. Menguji apakah data-data penting yang terkandung di dalam pesan sudah terenkripsi dengan aman jika dilakukan proses penyadapan terhadap pesan.

5.4 Kasus Uji

Pengujian dibagi menjadi 3 bagian yaitu pengujian protokol, pengujian fungsionalitas perangkat lunak simulasi serta pengujian

penyadapan pesan. Dalam pengujian protokol, diuji kesesuaian antara protokol *SMS-Banking* yang dibuat dengan tujuan protokol. Pengujian fungsionalitas perangkat lunak simulasi dilakukan dengan memeriksa hasil pesan yang dibangkitkan oleh *server* maupun klien baik untuk fase aktivasi dan fase transaksi. Pada pengujian penyadapan pesan dilakukan penyadapan pesan dengan menggunakan sebuah telepon seluler.

5.5 Pengujian Protokol

5.5.1 Kerahasiaan

Protokol *SMS-Banking* yang dibuat, sudah mengaplikasikan algoritma asimetri pada fase aktivasi dan algoritma simetri pada fase transaksi untuk mengenkripsi data-data penting milik klien dan *server*. Dalam pertukaran kunci simetri juga digunakan algoritma Diffie Hellman yang dapat menambah tingkat kerahasiaan dalam proses pertukaran kunci simetri. Oleh karena itu, tujuan kerahasiaan pesan sudah dipenuhi oleh protokol.

5.5.2 Otentikasi

Pada fase aktivasi, pihak *server* dapat mengotentikasi klien dengan memeriksa keseseuaian antara PIN, kode aktivasi, serta kode nasabah, sedangkan pada fase transaksi, pihak server dapat memeriksa kesesuaian antara PIN, kode nasabah serta nomor urutan yang ada. Selain itu, pada protokol juga digunakan algoritma asimetri dengan kunci publik dan kunci privat milik server dan klien, serta digunakan juga algoritma simetri. Penggunaan kedua algoritma tersebut digunakan untuk mengotentikasi server atau klien.

5.5.3 Integritas

Untuk memenuhi salah satu tujuan protokol yaitu integritas data, maka protokol mengaplikasikan tanda tangan digital. Dengan tanda tangan digital tersebut, dapat diperiksa apakah pesan yang diteima masih asli atau sudah tidak asli lagi.

5.5.4 Nirpenyangkalan

Protokol *SMS-Banking* yang dibuat menggunakan tanda tangan digital dengan menggunakan fungsi hash. Pada tanda tangan digital tersebut digunakan algoritma kunci publik sehingga baik penerima maupun pengirim pesan mempunyai pasangan kunci masing-masing. Selain itu, protokol *SMS-Banking* yang dibuat juga menggunakan algoritma kunci publik pada fase aktivasi. Karena kedua hal tersebut, tujuan protokol yaitu nirpenyangkalan sudah dipenuhi oleh protokol.

5.6 Pengujian Fungsional Perangkat Lunak

Hasil pengujian fungsional perangkat lunak untuk fase aktivasi menunjukkan bahwa perangkat lunak klien telah berhasil membangkitkan pesan fase aktivasi dengan baik. Selain itu, perangkat lunak *server* juga telah berhasil membangkitkan pesan balasan sesuai dengan pesan yang diterima dari klien. Untuk hasil pengujian fungsional perangkat lunak untuk fase transaksi menunjukkan bahwa perangkat lunak klien telah berhasil membangkitkan pesan fase transaksi dengan baik. Selain itu, perangkat lunak *server* juga telah berhasil membangkitkan pesan balasan sesuai dengan pesan yang diterima dari klien. Dari hasil-hasil pengujian tersebut, dapat diambil kesimpulan bahwa fungsionalitas perangkat lunak telah berjalan dengan baik.

Jumlah pesan SMS yang dibutuhkan dalam fase aktivasi dan fase transaksi baik *server* maupun klien adalah lebih dari 2 buah. Jumlah pesan SMS yang diperlukan dalam fase aktivasi untuk klien adalah sebanyak 4 pesan SMS, sedangkan untuk *server* sebanyak 4 pesan SMS. Jumlah pesan fase transaksi untuk klien adalah sebanyak 3 pesan SMS, sedangkan untuk *server* sebanyak 5 pesan SMS. Dari data-data tersebut dapat disimpulkan bahwa protokol *SMS-Banking* yang dibuat cukup tinggi dalam hal jumlah pesan SMS yang digunakan.

5.7 Pengujian Penyadapan

Berdasarkan hasil pengujian, data-data penting yang terdapat pada pesan aktivasi dan transaksi yang dikirim baik oleh klien maupun server, sulit dibaca oleh penyadap. Hal ini dapat dinyatakan bahwa proses enkripsi pada data-data yang penting pada pesan akan mempersulit proses penyadapan.

6. Kesimpulan

1. Protokol *SMS-Banking* yang dirancang telah terbukti dapat diimplementasikan dengan baik pada perangkat lunak simulasi yang dibuat. Baik perangkat lunak yang diimplementasikan pada klien, SMS *gateway* dan *server* telah berjalan dengan baik.
2. Panjang pesan hasil enkripsi yang dihasilkan oleh algoritma RSA relatif lebih panjang dibandingkan dengan pesan hasil enkripsi oleh algoritma Rijndael. Selain itu, waktu yang dibutuhkan oleh algoritma RSA dalam

proses enkripsi relatif lebih lambat dibanding dengan algoritma Rijndael.

3. Penggunaan SMS untuk layanan perbankan memang lebih memakan biaya dibanding dengan menggunakan internet. Namun, penggunaan SMS untuk layanan perbankan lebih baik dibanding dengan menggunakan GPRS dalam daerah yang tidak memiliki koneksi internet.
4. Penggunaan *sequence number* dapat menghindari penggunaan kembali pesan yang telah disadap oleh penyadap sehingga tingkat keamanan pesan pun bertambah.
5. Pada pembangunan aplikasi pada sistem operasi yang berbasis Microsoft Windows Mobile 5.0, Microsoft menyediakan *software development kit* yang sangat membantu para pengembang.
6. Pada PDA yang berbasis Windows Mobile 5.0 dapat dibuat SMS *gateway* yang memanfaatkan pemrograman socket dan fasilitas penerimaan dan pengiriman SMS.

7. Saran

1. Pesan SMS yang dikirim sebaiknya dikompresi sehingga dapat mengurangi panjang SMS. Dengan mengurangi panjang SMS, diharapkan biaya yang digunakan untuk mengirim SMS dapat berkurang.
2. Untuk lebih mengetahui tingkat keamanan protokol *SMS-Banking* yang telah dirancang, dapat diimplementasikan protokol tersebut pada sistem perbankan yang *real*. Hal tersebut dimaksudkan untuk dapat melihat kelayakan protokol *SMS-Banking* yang dibuat untuk digunakan di dunia nyata.
3. Dalam menggunakan algoritma pertukaran kunci Diffie Hellman, sebaiknya digunakan nilai p, q, x dan y yang bernilai besar agar proses pertukaran kunci dapat berlangsung lebih aman.
4. Untuk pengembangan protokol selanjutnya, dapat digunakan kode nasabah yang bersifat sementara sehingga tingkat keamanan protokol dapat lebih baik.
5. Untuk pengembangan selanjutnya, dapat dibuat aplikasi telepon seluler yang berbasis Java, Symbian, Iphone, dan Windows Mobile yang terbaru agar *platform* yang didukung menjadi semakin luas.

DAFTAR PUSTAKA

[REA08] Marguerite Reardon (2008). Americans Text More Than They Talk <http://news.cnet.com/8301-1035_3-10048257-94.html> Tanggal Akses: 10 Maret 2009, 15:25.

[SIN08] Roike Sinaga (2008). Lebaran, Saatnya Operator Seluler Menangguk Untung. <http://www.antara.co.id/arc/2008/8/31/lebaran-saatnya-operator-seluler-menangguk-untung> Tanggal Akses: 10 Maret 2009, 15:30.

[ALM07] Luciana Spica Almilia, Antomy Nova Giarta (2007). Perspektif Nasabah Perbankan atas kehadiran *SMS banking* dan *WAP banking* sebagai sistem informasi perbankan yang bernilai tambah.

[STR08] Pieter Streicher (2008). *SMS* Phising On The Increase. <http://www.bizcommunity.com/Article/196/78/26041.html> Tanggal Akses: 10 Maret 2009, 15:45.

[PAN04] Denis Pankratov, Dmitri Kramarenko (2004). SMS spoofing – Q&A with CCRC staff.

[CHI06] Kelvin Chikomo, Ming Ki Chong, Alapan Arnab, Andrew Hutchison (2006). *Security of Mobile Banking*.

[EMM07] Abunyang Emmanuel (2007). Mobile Banking in Developing Countries: Secure Frame work for Delivery of SMS-banking Services.

[KOH04] Karmendra Kohli (2004). SMS in Banking Mitigating the Risks. Paladion Knowledge Series.

[PES99] Lauri Pesonen (1999). GSM Interception.

[BUD08] Budiono (2008). Penerapan Tanda Tangan Digital Untuk Otentikasi *SMS-Banking*.

[PER08] Rangga Wisnu Adi Permana (2008). Implementasi Algoritma RC6 Untuk Enkripsi SMS Pada Telepon Selular.

[SCH96] Bruce Schneier (1996). Applied Cryptography 2nd. John Wiley & Sons.

[MUN09] Rinaldi Munir (2009). IF3058 Kriptografi.

[MEH03] Subhash Mehta (2003). Academic's Dictionary Of Computers. Academic India Publishers.