

BAB I

PENDAHULUAN

1.1 Latar Belakang

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 penggunaannya 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].

1.2 Rumusan Masalah

Masalah-masalah yang akan dikaji dan diselesaikan dalam Tugas Akhir ini meliputi:

1. Bagaimana mengimplementasikan teknologi tanda-tangan *digital* pada pesan SMS untuk otentikasi *SMS-Banking* dengan menggunakan algoritma RSA.
2. Bagaimana menguji keamanan transaksi simulasi *SMS-Banking* dengan menggunakan teknologi tanda-tangan *digital* dan algoritma RSA.

1.3 Tujuan

Tujuan utama yang ingin dicapai dalam pelaksanaan Tugas Akhir ini adalah menerapkan algoritma RSA untuk otentikasi *SMS-Banking*. Adapun beberapa tujuan lain yang ingin dicapai dalam pelaksanaan Tugas Akhir ini adalah sebagai berikut:

1. Memahami dan mempelajari sistem transaksi perbankan *online* dengan menggunakan SMS.
2. Mengkaji penggunaan algoritma RSA yang nantinya akan digunakan dalam pembentukan tanda-tangan *digital* pada aplikasi simulasi *SMS-Banking*.
3. Membangun perangkat lunak simulasi yang mengimplementasikan tanda-tangan *digital* pada perangkat *mobile* dan komputer *server* yang telah terhubung dengan GSM *modem*.
4. Menguji tingkat keamanan otentikasi yang bisa diberikan oleh teknologi tanda-tangan *digital* untuk *SMS-Banking*.

1.4 Batasan Masalah

Batasan masalah yang didefinisikan dalam pelaksanaan Tugas Akhir ini adalah:

1. Proses transaksi perbankan melalui SMS dilakukan dengan menggunakan simulasi antara telepon seluler dengan komputer *server* yang terhubung dengan *GSM modem*.
2. Titik berat Tugas Akhir adalah otentikasi pesan *SMS-Banking* bukan transaksi *SMS-Banking* secara keseluruhan.
3. Proses otentikasi pesan transaksi SMS dilakukan oleh perangkat lunak yang dibangun diatas komputer *server* yang terhubung dengan *GSM Modem*.
4. Pengguna tidak mengetikkan pesan SMS transaksi yang ada, namun hanya menggunakan menu yang ada pada aplikasi di handphone.
5. Kunci publik yang dihasilkan tidak termasuk dalam sertifikasi *digital* yang ditetapkan oleh pemegang otoritas sertifikasi (*Certification Authority* atau *CA*).

1.5 Metodologi

Dalam penyusunan tugas akhir ini digunakan metodologi sebagai berikut:

1. **Studi literatur**, dilakukan dengan cara mempelajari literatur-literatur baik yang berupa buku (*textbook*), jurnal dan artikel ilmiah, maupun *website* yang berhubungan dengan penggunaan *digital signature* untuk keamanan sebuah pesan tertentu dengan menggunakan algoritma RSA.
2. **Analisis masalah**, dilakukan dengan menganalisis cara mengimplementasikan *digital signature* pada sebuah pesan SMS yang dikirimkan melalui telepon seluler tertentu dan diterima oleh sebuah komputer yang terhubung dengan *GSM modem* sehingga dapat dilakukan verifikasi pesan transaksi.
3. **Perancangan perangkat lunak**, yaitu dengan cara membuat desain prototipe perangkat lunak yang dapat mengimplementasikan hasil analisis masalah di atas.

4. **Implementasi perangkat lunak**, dilakukan berdasarkan hasil perancangan prototipe perangkat lunak.
5. **Pengujian perangkat lunak**, dilakukan dengan cara menjalankan perangkat lunak dengan input berupa pesan SMS yang merepresentasikan transaksi perbankan tertentu. Kemudian, SMS tersebut akan diverifikasi oleh perangkat lunak yang berjalan diatas komputer yang terhubung dengan GSM *modem*.
6. **Analisis hasil dan penarikan kesimpulan**, yaitu memaparkan tingkat keamanan yang didapatkan dari penerapan *SMS-Banking* dengan menggunakan *digital signature* dan menarik kesimpulan dari hasil pemaparan tersebut.