BAB I PENDAHULUAN

1. Latar belakang

Short Message Service, atau SMS lebih dikenal sebagai suatu pelayanan yang memungkinkan pengiriman pesan text melalui jaringan seluler. Pesan bisa disimpan di jaringan sampai pesan-pesan tersebut dikumpulkan oleh perlengkapan terminal si penerima (seperti *mobile phone* atau device yang bisa terhubung ke jaringan). SMS awalnya didesain sebagai bagian dari *Global System for Mobile communications* (*GSM*), namun dewasa ini telah tersedia pada sebuah cakupan standar jaringan yang luas seperti Code Division Multiple Access (*CDMA*). Walaupun SMS awalnya dimaksudkan untuk notifikasi pengguna terhadap pesan *voicemail*, SMS sekarang telah menjadi suatu alat terkenal terkait komunikasi oleh individu dan bisnis. Dunia Bank sekarang tengah gencar-gencarnya menggunakan SMS untuk memimpin beberapa pelayanan banking-nya. Misalnya, klien bisa mengirim query/mempertanyakan saldo banknya melalui SMS ataupun memimpin pembayaran secara mobile. Kebanyakan orang terkadang saling menukarkan informasi konfidental seperti *password* atau data sensitif secara personil.

SMS menyediakan banyak kenyamanan dalam kehidupan sehari-hari namun apakah benar-benar aman? Saat informasi yang sifatnya sensitif dipertukarkan menggunakan SMS, sangatlah krusial untuk melindungi isi SMS tersebut dari seseorang serta menjamin keaslian pesan berasal dari pengirim yang sah. Pesan SMS dikirim melalui suatu mekanisme *store and forward* ke suatu *Short Message Service Centre* (*SMSC*), yang akan berusaha untuk mengirimkan pesan ke penerima dan mengirim ulang bila pengguna tidak dapat dijangkau pada waktu itu. Transmissi SMS diantara SMSC dan phone melalui *Signalling System Number 7* (*SS7*) di dalam framework GSM MAP (Mobile Application Part). Permasalahan yang muncul dengan *GSM MAP* yakni tidak terenkripsinya protokol dimana hal ini membolehkan pegawai jaringan seluler yang mempunyai hak akses ke jaringan SS7 untuk mencuri informasi atau mengubahnya/memodifikasi pesan SMS.

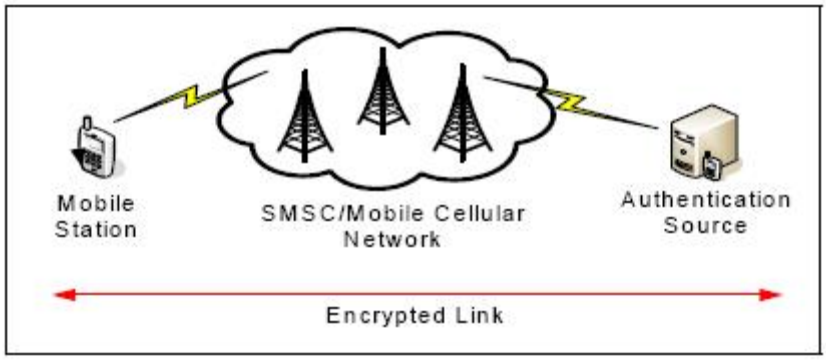
Sehingga kebutuhan akan informasi yang mobile juga menjadi latar belakang bagi perkembangan teknologi proteksi komunikasi data. Tidak jarang ditemui adanya perilaku kriminal yang mencoba masuk ke celah-celah komunikasi data ini.

SMSSec, sebagai end to end protokol untuk keamanan komunikasi data, diklaim dapat mengamankan mekanisme pertukaran data pada aplikasi SMS. Oleh karena itu, pada tugas akhir ini perlu dilakukan implementasi protokol SMSSec pada sebuah aplikasi mobile internet berbasis JAVA, dan nantinya akan dilakukan analisis kinerja terhadap implementasi SMSSec pada sebuah aplikasi SMS untuk melihat sejauh mana protokol ini dapat mengamankan mekanisme pertukaran data tersebut.

2. Perumusan masalah

Protokol SMSSec memiliki dua fase handshake. Handshake kali pertama dengan menggunakan *kriptografi kunci asimetrik* (RSA (***R***on Rivest, Adi ***S***amir, dan Leonard ***A***dleman) 2048-*bits*) dan handshake ke-*n* dengan menggunakan *kriptografi kunci simetrik* (AES (AES) 256-*bits*) serta menyertakan fungsi hash HMAC_SHA256 untuk meng-otentikasi pesan.

end system yang dimaksud adalah [6]:



Gambar 1.2 End System

Adapun perumusan masalah dari tugas akhir ini, yakni:

1. Bagaimana implementasi pendekatan protokol SMSSec pada sebuah aplikasi mobile Internet berbasis JAVA.
2. Bagaimana kinerja pendekatan SMSSec dalam menambahkan fitur keamanan pada sebuah aplikasi SMS, meliputi kinerja aplikasi yang mengadopsi kerja protokol SMSSec (hanya 1 handshake) yakni respon time dan penggunaan memory selama proses serta kinerja komponen pembangun protokol SMSSec yakni avalanche effect, panjang data output, ketahanan terhadap brute force attack dan ketahanan terhadap serangan *eavesdropping* atau *modification*.

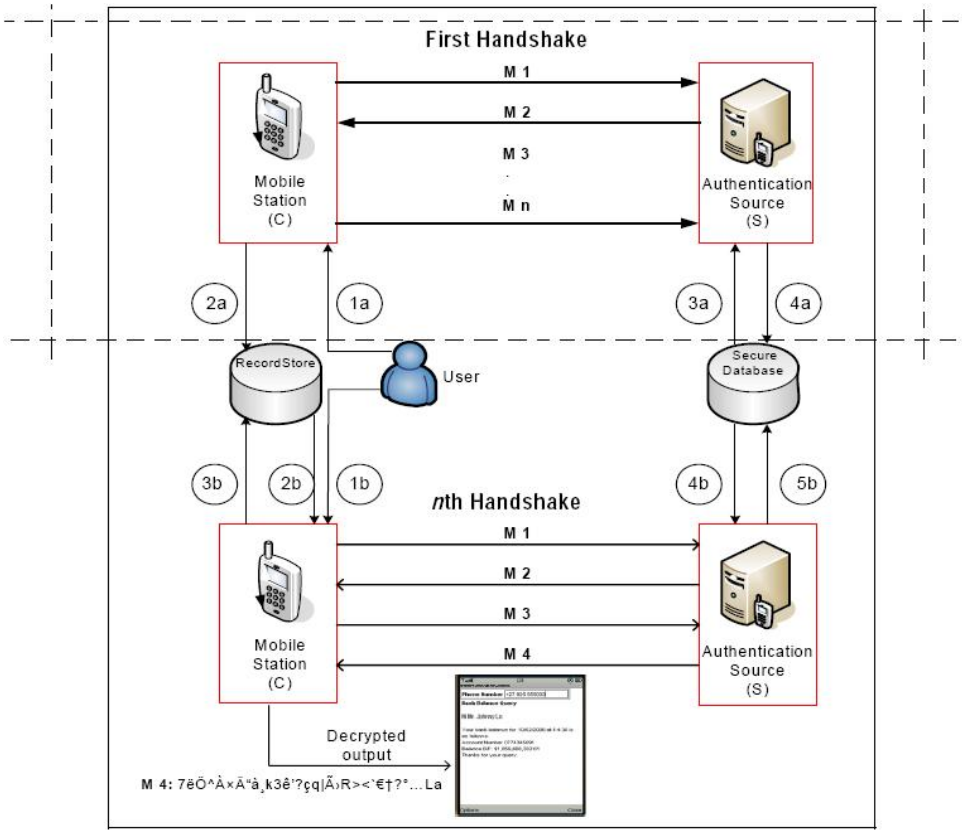
3. Batasan masalah

Berikut adalah batasan-batasan yang ditentukan untuk aplikasi yang dibangun, yakni:

1. Implementasi akan dilakukan pada simulator untuk HP dengan memakai bahasa pemrograman yang *kompatibel* dengan *simulator* tersebut, yakni Java (J2SE/J2ME), dan Database yang digunakan adalah MySQL.
2. Aplikasi yang dibangun melibatkan dua pihak, yakni pihak nasabah yang didefinisikan sebagai klien dan pihak bank yang didefinisikan sebagai server. Diasumsikan klien sudah terdaftar di bank dan sudah memiliki kunci public dan private, kunci private sudah digenerate di server.
3. *Recordstore* dan *Database* untuk PIN diasumsikan di *kanal* yang aman.
4. Di tugas akhir ini tidak membahas/memfokuskan pada USSD namun terkait murni pada SMS. Tidak membahas/memfokuskan pada arsitektur GSM, SS7, SMSC, dan GSM MAP.
5. Kunci RSA yang digunakan adalah 2048 bits, kunci AES yang digunakan adalah 256 bits, fungsi Hash yang digunakan adalah HMAC_SHA256. Untuk simetrik chiper, pilihan algoritmanya adalah AES karena kecepatannya, efisiensi dan standar(d)isasi. Untuk asimetrik chiper, pilihan algoritma yang digunakan adalah RSA. chiper RSA telah dipercaya selama beberapa tahun dan sampai sekarang masih digunakan untuk mengamankan aplikasi e-commerce. seiring technologi berkembang dalam memfaktorkan RSA primes, panjang kunci yang paling aman untuk 20 tahun ke depan adalah 2048 bit. bila RSA dibandingkan dengan ECC (Elliptic Curve Cryptography) maka tampak sekali ECC menawarkan keamanan data dengan ukuran kunci yang pendek dengan demikian mengurangi processing overhead. namun ECC telah dipatenkan oleh beberapa orang dan perusahaan di dunia, misalnya perusahaan Canadian, Certicom Inc. memegang 130 hak patent terkait dengan ECC dan kriptografi publik pada umumnya. Sedangkan HMAC dengan dasar fungsi hash yang disebut SHA_256 dipilih karena akhir-akhir ini adanya attack pada collision pada SHA1 dan berdasarkan rekomendasi oleh National Institute of Standards and Technology yakni SHA1 tidak dipakai lagi menjelang tahun 2010. karena itu, dengan dipilihnya suatu fungsi hash yang akan bertahan/berlangsung sampai tahun 2010, HMAC diperlukan untuk melindungi digest dari collision partial dan serangan length extension.
6. Tidak mendefinisikan session identifier dan penggunaan nomor hp.

7. Handshake yang terjadi hanya satu yakni handshake pertama yang melibatkan juga handshake ke-n di dalam sub handshake-nya. Hal ini dikarenakan aplikasi yang dibangun tidak menyertakan two factor authentication atau web based aplication.

Berikut adalah gambar dari sistem yang akan dibangun dengan mengadopsi protokol SMSSec yakni menggunakan satu kali handshake.



Gambar 1.3 Mekanisme SMSSec teradopsi

4. Tujuan Penelitian

Adapun tujuan penelitian dari tugaas akhir ini antara lain:

1. Melakukan implementasi pendekatan protokol SMSSec (disimulasikan di laptop).
2. Menganalisis kinerja pendekatan protokol SMSSec pada aplikasi SMS, meliputi *k*inerja aplikasi yang mengadopsi kerja protokol SMSSec (hanya 1 handshake) yakni respon time dan penggunaan memory selama proses serta *k*inerja komponen pembangun protokol SMSSec yakni avalanche effect,

panjang data output, ketahanan terhadap brute force attack dan ketahanan terhadap serangan *eavesdropping* atau *modification*.

5. Metodologi perumusan masalah

Tahap-tahap yang dilakukan adalah:

1. Studi literatur, hal ini dilakukan untuk memecahkan rumusan permasalahan berdasarkan referensi dan mengumpulkan data terkait dengan perumusan masalah, yang berkaitan dengan
   - Wireless messaging.
   - Protokol untuk sms.
   - Kriptografi Asimetrik (RSA (2048-bits)), Simetrik (AES (256-bits)), dan Hash (HMAC_SHA256).
   - Aplikasi SMS Banking pada mobile phone berbasis JAVA.
2. Membuat aplikasi SMS Banking.
3. Pengimplementasian dari rancangan yang telah dibuat dan melakukan uji coba di simulator terhadap studi ini sesuai dengan batasan masalah.
4. Mengambil simpulan dari studi dan simulasi yang telah dilakukan.