Penerapan Kriptografi
dalam Sistem Keamanan SMS Banking

Biyan Satyanegara / 13508057
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18057@students.if.itb.ac.id

***Abstract*— Makalah ini berisi tentang penerapan kriptografi dalam sistem keamanan SMS Banking. SMS Banking adalah layanan perbankan yang menggunakan teknologi telkomunikasi SMS agar nasabah bank dapat melakukan berbagai transaksi dimanapun berada. Makalah ini dibuat dengan tujuan mengetahui seberapa aman transaksi SMS banking yang saat ini sering dilakukan terutama di Indonesia. Selain itu makalah ini dibuat untuk mengetahui aplikasi algoritma kriptografi untuk dunia nyata dalam hal ini pengaplikasian dilakukan pada layanan SMS Banking. Kesimpulan dari hasil analisis adalah Penerapan algoritma kriptografi merupakan faktor yang penting dalam sistem keamanan SMS banking.**

***Kata kunci* — algoritma, kriptografi, keamanan, dan sms banking.**

I. PENDAHULUAN

Kebutuhan akan transaksi dan teknologi telekomunikasi saat ini berkembang cukup pesat. Banyak sekali alat komunikasi yang keluar di pasaran tiap bulannya dengan menawarkan fitur-fitur yang baru. Di sisi lain perkembangan teknologi komunikasi ini menimbulkan kebutuhan akan tersedianya informasi yang cepat. Saat ini manusia dapat berkomunikasi dengan cepat melalui telepon seluler. Selain itu pertukaran data informasi saat ini dapat dilakukan secara mudah dengan menggunakan internet. Hal inilah yang menyebabkan banyaknya layanan transaksi terutama di bidang jasa yang menggunakan media-media telekomunikasi. Salah satu layanan telekomunikasi yang sering digunakan dan sedang berkembang di Indonesia adalah SMS banking.

SMS Banking adalah penggunaan layanan transaksi perbankan dengan menggunakan sarana telekomunikasi yaitu SMS. Saat ini pelanggan bank dapat melakukan berbagai macam transaksi perbankan seperti : cek saldo, transfer, pembayaran dll dimanapun ia berada dengan menggunakan fitur SMS pada telepon genggam yang dimilikinya. Pengguna hanya perlu memasukkan nomor PIN pada telepon genggam yang dimiliknya untuk melakukan semua fitur perbankan yang ditawarkan oleh layanan SMS banking. Namun banyaknya pelanggan yang menggunakan layanan SMS banking tidak diimbangi dengan faktor keamanan yang ada pada layanan tersebut. Sampai saat ini kejahatan terhadap layanan SMS banking masih sering terjadi. Layanan ini menjadi rentan kejahatan dikarenakan banyaknya data pribadi yang dimasukkan pelanggan ke dalam konten SMS, mulai dari nomor PIN, nomor rekening dll. Kejahatan yang terjadi biasanya dilakukan dengan cara penyadapan pada saat pengiriman data dari telepon seluler. Data menjadi sangat rentan disadap terlebih lagi terdapat beberapa layanan SMS banking yang tidak menggunakan enkripsi pada konten SMS. Enkripsi dapat digunakan sebagai faktor keamanan tambahan pada SMS banking. Isi sms sulit untuk dibaca karena isi sms telah dimodifikasi sedemikian rupa sehingga tidak bisa dibaca jika tidak mendapatkan kunci enkripsi.

Kriptografi memiliki beberapa algoritma yang dapat digunakan untuk mengamankan sebuah data atau informasi. Algoritma kriptografi ini dapat diterapkan dalam pengamanan layanan SMS banking tersebut. Konten sms dapat dienkripsi dengan salah satu algoritma maupun kombinasi dari beberapa alogritma kriptografi sehingga isi SMS yang berisi data pribadi pelanggan bank tidak dapat dibaca dengan mudah oleh penyadap.

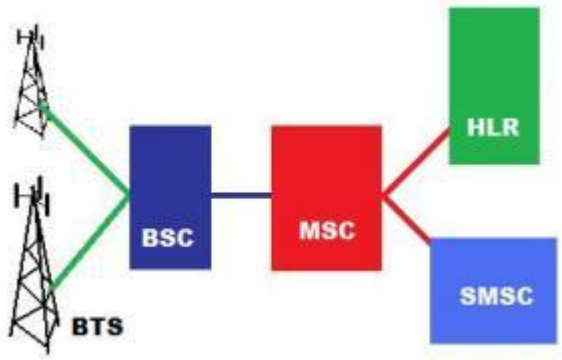
II. LANDASAN TEORI

A. Cara Kerja SMS

Short Message Service (SMS) adalah layanan dasar telekomunikasi seluler, yang tersedia baik di jaringan GSM maupun CDMA. Sebagai layanan dasar, service sms dapat digunakan pada semua jenis hand phone (HP). Setiap SIM card dari sebuah operator yang diaktifkan hampir dipastikan dapat langsung dapat digunanakan untuk sms, karena SIM card akan otomatis menyediakan setting service center di HP tersebut.

Untuk mengetahui proses pengiriman sms berlangsung, perlu mengetahui arsitektur jaringan yang dipakai. Di Indonesia ada 2 macam teknologi jaringan seluler yang cukup populer, yaitu GSM dan CDMA. Pembahasan ini akan fokus pada arsitektur jaringan GMS karena layanan jaringan yang banyak digunakan adalah GSM.

Dalam jaringan GSM umumnya ada beberapa perangkat pokok diantaranya BTS, BSC, MSC/VLR, HLR dan SMSC. Berikut ini penjelasan masing-masing perangkat :

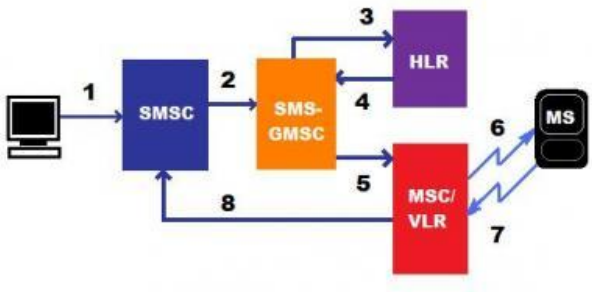


Gambar 1. Arsitektur Jaringan GSM

1. Base Transceiver Station (BTS)
   BTS berfungsi sebagai perangkat tranceiver untuk melakukan komunikasi dengan semua handset (MS) yang aktif dan berada dalam area cakupannya (cell). BTS melaksanakan proses modulasi/demodulasi sinyal, equalisasi sinyal dan pengkodean error (error coding). Beberapa BTS dapat terhubung dengan sebuah BSC (Base stasion Controller), sementara itu radius cakupan dari suatu cell berkisar antara 10 sampai 200 m untuk cell terkecil hinggal beberapa kilometer untuk cell terbesar. Sebuah BTS biasanya dapat melayani 20–40 komunikasi panggilan secara bersamaan.
2. Base Station Controller (BSC)
   BSC menyediakan fungsi pengaturan pada beberapa BTS yang dikendalikannya. Dinataranya fungsi handover, konfigurasi cell site, pengaturan sumber daya radio, serta tuning power dan frekuensi pada suatu BTS.
   BSC merupakan simpul (konmsentrator) untuk menghubungkan dengan core network. Dalam jaringan GSM umumnya sebuah BSc dapat mengatur 70 buah BTS.
3. Mobile Switching Center (MSC) and Visitor Location Register (VLR)
   MSC berfungsi melakukan fungsi switching dan bertanggung jawab untuk melakukan pengaturan panggilan, call setup, release, dan routing. MSC juga melakukan fungsi billing (terhubung ke billing system) dan sebagai gateway ke jaringan lain. VLR berisi informasi user yang bersifat dinamis yang sedang “attach” berada pada jaringan mobile, termasuk letak geografis. Biasanya VLR terintegrasi dengan MSC.
   Dari MSC sebuah jaringan seluler berkomunikasi dengan jaringan luar, misalnya : jaringan telepon rumah/Public Switched Telephone Network (PSTN), jaringan data Integrated Services Digital Network (ISDN),
   Circuit Switched Public Data Network (CSPDN), dan Packet Switched Public Data Network (PSPDN).
4. Home Location Register (HLR)
   HLR adalah perangkat yang berisi data detail untuk tiap subscriber. Sebuah HLR umumnya mampu berisi ribuan sampai jutaan data pelanggan. Informasi yang ada di HLR antara lain Mobile Station ISDN Number (MSISDN), International Mobile Subscriber Identity (IMSI), profile service subscriber,dll. Untuk komunikasi dengan elemen jaringan lain, HLR menggunakan protokol MAP (Mobile Application Part)
5. Short Message Service Center (SMSC)
   SMSC mempunyai peran penting dalam arsitektur sms. SMSC berfungsi menyampaikan pesan sms antar Mobile Station(MS)/ HP, dan juga melakukan fungsi store-and-forwarding sms jika nomor penerima sedang tidak dapat menerima pesan. Didalam jaringanya sebuah operator dapat mempunyai lebih dari satu perangkat SMSC, sesuai besar trafik sms jaringan tersebut. SMSC dapat berkomunikasi dengan elemen lain seperti MSC, dan HLR dengan menggunakan protokol MAP. Seiring berkembangnya layanan, SMSC juga dapat berkomunikasi dengan server aplikasi menggunakan sebuah protokol yang cukup pupuler yaitu, Short Message Peer tio Peer Protocol (SMPP).

Ada dua macam layanan dasar SMS:

a. SMS Mobile Terminating (SMS MT)
   SMS MT adalah pengiriman SMS dari SMSC ke MS. Untuk pegiriman SMS ini akan disediakan informasi pengiriman, baik delivery report untuk SMS yang berhasil maupun failure report untuk pengiriman yang gagal karena sebeb tertentu, sehingga memungkinkan SMSC untuk melakukan pengiriman ulang.



Gambar 2. Diagram Alir SMS

Diagram Alir SMS Mobile Terminating.

1. A (misal: aplikasi) mengirim pesan ke SMSC
2. SMSC mengirimkan pesan ke SMS–GMSC.
3. SMS–GMSC menginterogasi HLR untuk informasi routing.
4. HLR membalas informasi routing ke SMS-GMSC.
5. SMS-GMSC meneruskan pesan ke MSC/VLR.
6. MS di-paging dan koneksi terbentuk antara MS dan network, sebagaimana dalam setup

pangilan normal.
(Dengan demikian posisi MS diketahui dan apakah MS boleh berada dalam network / proses otentikasi).

7. Jika otentikasi berhasil, MSC/VLR mengirim pesan sms tersebut ke MS. SMS dikirim melalui kanal signaling SDCCH)
8. Jika pengiriman berhasil, delivery report dikirim dari MSC/VLR ke SMSC. Namun jika tidak, MSC/VLR akan menginformasikan ke HLR, dan failure report dikirim ke SMS–C. Pada kasus pengiriman yang gagal, HLR dan VLR akan mendapat informasi "Messages waiting" yang menunjukkan ada pesan di SMSC yang menunggu untuk dikirimkan ke MS. Informasi di HLR terdiri dari list SMSC pengirim pesan, sedangkan di VLR terdapat "flag" yang menunjukkkan apakah list pesan dalam keadaan kosong atau tidak. Jika MS available dan siap menerima pesan, maka HLR akan memberitahu SMSC.

b. SMS Mobile Originating (SMS MO)
SMS MO adalah proses pengiriman SMS dari MS ke SMSC. Jika SMS terkirim ke MS akan mendapat report "message sent", sementara jika gagal MS report yang terlihat adalah "sending failed".

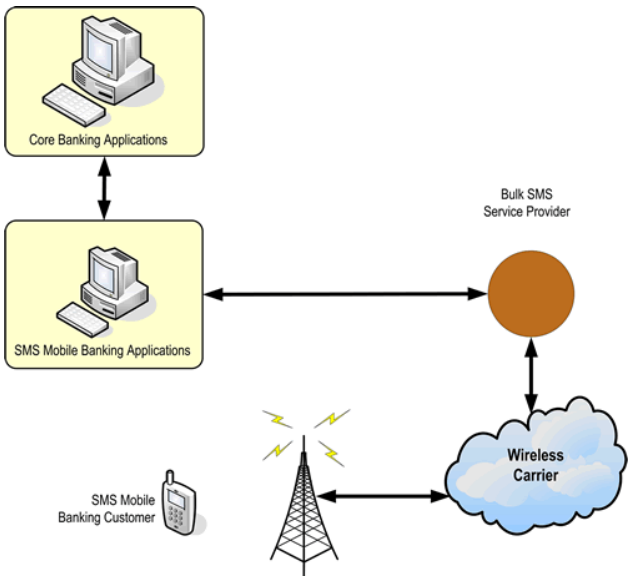
Gambar 3. SMS mobile Originating (SMS MO)

Keterangan Diagram alir SMS MO:

1. MS membuat koneksi ke jaringan, sebagaimana dalam setup panggilan normal.
2. Jika otentikasi berhasil, MS akan mengirim SMS ke SMSC melalui MSC/VLR. Selanjutnya SMSC akan meneruskan SMS ke tujuan.

B. Cara Kerja SMS Banking

Untuk memanfaatkan layanan sms banking pengguna harus berlangganan ke operator telepon agar dapat mengirimkan sms dengan kode standar untuk nomor penyedia layanan bulk.

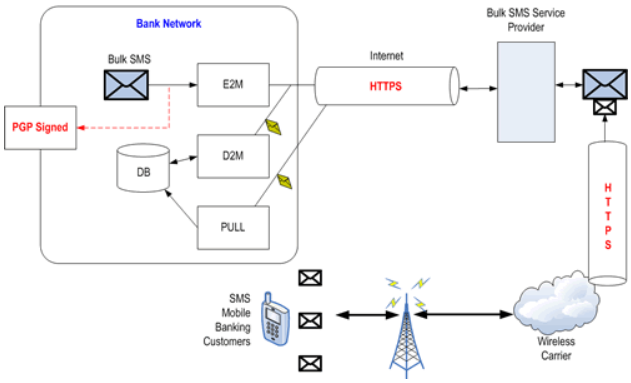


Gambar 4. Arsitektur SMS Banking

Service provider akan meneruskan pesan kepada aplikasi mobile banking. Aplikasi mobile banking ini terhubung dengan server pusat bank (yang menyimpan informasi akun user) untuk melayani permintaan servis yang dibuat user. Respon akan dikirmkan oleh aplikasi mobile banking ke bulk service provider yang akan mengirimkan balik ke pengguna menggunakan SMS balasan. Ada dua cara bank berkomunikasi dengan user menggunakan SMS :

1. Bank secara aktif mengirimkan data ke pelanggan untuk merespon setiap transaksi. Contoh : transfer dari akun ke akun lain, kredit gaji dan pesan promosi. Data ini dikirmkan dengan menggunakan dua cara : email to mobile E2M dna database to mobile (D2M)
2. Bank mengirimkan data untuk merespon query pelanggan secara spesifik seperti penampilan akun tabungan secara detail

Berikut Arsitektur jaringan untuk kemanan transaksi dengan sms banking

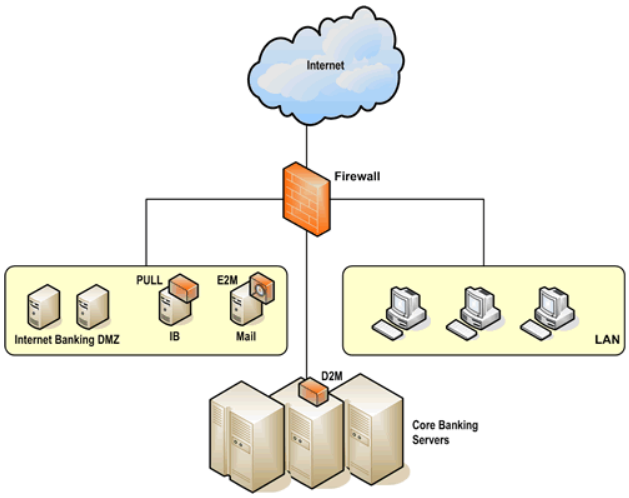


Gambar 5. Skema jaringan keamanan untuk SMS Banking

Pada gambar 5 jalur antara SSL link dengan service provider, mobile banking application dengan service provider, dan service provider dengan wireless carrier

memastikan kerahasiaan data. Email yang dikirimkan oleh bank telah dienkripsi dan perlu di sign in untuk memastikan kerahasiaan dan integritas data.

Pada gambar 6 akan ditunjukkan tempat penyimpanan SMS banking pada infrastruktur sebuah bank.



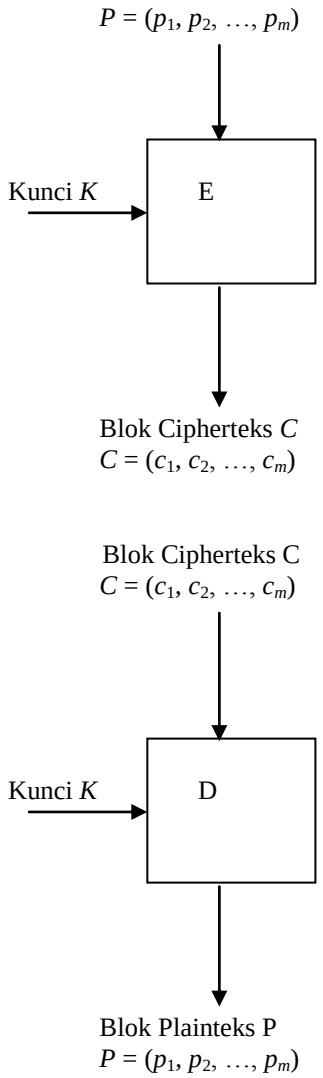
Gambar 6. Diagram penyimpanan SMS banking pada infrastruktur bank

Pada gambar 6, komponen E2M ditempatkan pada mail server yang telah ada pada internet banking DMZ. Komponen tersebut menyimpan pesan email dari email server yang akan diteruskan ke service provider dengan format yang sesuai SSL link. Komponen D2M ditempatkan di dalam core-banking yang akan terus memperbaharui database untuk sebuah event yang terjadi. Kemudian komponen PULL akan ditempatkan pada server internet banking ketika komponen tersebut berhasil menerima pesan dari bulk service provider melalui SSL link pada internet.

C. Algoritma Kriptografi Modern

Algoritma kriptografi memiliki berbagai macam jenis dan aplikasinya. Algoritma kriptografi dapat dibagi menjadi dua macam yaitu algoritma kriptografi sederhana dan algoritma kriptografi modern. Pada pembahasan kali ini algoritma yang dibahas hanya algoritma kriptografi modern karena algoritma kriptografi modern dianggap memiliki tingkat keamanan tinggi. Hal ini disebabkan algoritma kriptografi modern beroperasi dalam bentuk bit sehingga tidak dapat dipecahkan dengan teknologi yang sederhana.

Salah satu algoritma kriptografi modern yang sering digunakan adalah algoritma block cipher. Metode block cipher adalah metode dengan membagi teks menjadi blok dengan jumlah atau panjang bit tertentu misalkan saja 128 bit. Untuk pesan yang lebih banyak dari itu pesan akan dibagi menjadi blok-blok pesan dengan ukuran yang sama dan menggunakan kunci yang sama pula. Skema enkripsi dan dekripsi pada cipher blok adalah sebagai berikut:



Gambar 7. Skema Enkripsi dan Dekripsi pada cipher blok

Beberapa algoritma cipher block yang digunakan dalam pengaplikasian keamanan jaringan adalah sebagai berikut :

1. Electronic Code Book (ECB)
   Electronic Code Book adalah metode pengenkripsian setiap blok cipherteks secara individual dan independen menjadi blok cipherteks dengan fungsi enkripsi tertentu, misalnya XOR, dan kunci tertentu. Jika panjang plainteks tidak habis dibagi dengan ukuran blok, maka blok terakhir yang berukuran lebih pendek daripada blok-blok lainnya maka akan ditambahkan bit-bit padding untuk menutupi kekurangan dari bit-bit blok tersebut misalnya dengan menambahkan bit 0 semua.
2. Cipher Block Chaining (CBC)
   Pada metode CBC setiap blok cipherteks bergantung tidak pada hanya bloknya saja namun juga pada keseluruhan blok plainteks sebelumnya karena hasil enkripsi blok yang sebelumnya dijadikan *feedback* untuk enkripsi blok yang sedang dikerjakan. Pada enkripsi blok pertama diperlukan blok semu yang disebut sebagai IV (*initialization vector*) yang pada pengerjaan tugas ini akan dibangkitkan secara acak

oleh program.Dan pada proses dekripsi, blok plainteks diperoleh dengan cara meng-*XOR*-kan IV dengan hasil dekripsi terhadap blok cipherteks pertama.

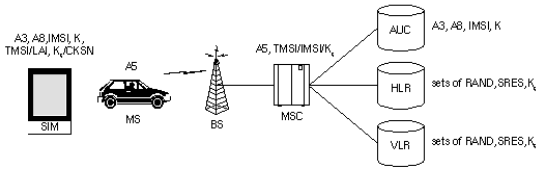
3. Cipher Feedback (CFB)
   Pada CFB metode yang digunakan sangatlah mirip dengan metode CBC. Hanya saja pada metode CFB data dienkripsikan lebih kecil daripada ukuran blok, pada pengerjaan tugas ini misalnya digunakan 8 bit(satu karakter setiap kali enkripsi dilakukan).
4. Output Feedback
   Pada metode OFB mirip dengan metode CFB, hanya saja dengan metode ini n-bit dari hasil enkripsi terhadap antrian disalin menjadi elemen posisi paling kanan di antrian. Proses Dekripsi dilakukan sebagai kebalikan dari proses enkripsi.

III. ANALISIS

A. Sistem Keamanan SMS Banking

Sistem keamanan pada sms banking terdiri dari beberapa aspek : subscriber identity authentication, subscriber identity confidentiality, signaling data confidentiality, and user data confidentiality.

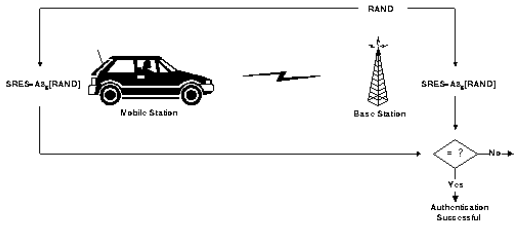
Mekanisme keamanan pada SMS banking diimplementasikan dalam tiga elemen sistem yang berbeda yaitu : Subscriber Identity Module (SIM), GSM handset atau MS, and jaringan GSM. SIM mengandung International Mobile Subscriber Identity (IMSI), kunci autentifikasi pelanggan (Ki), algoritma pembangkit ciphering key (A8), algoritma autentifikasi (A3) dan penggunaan PIN (personal identification Number). Pada GSM handset terdapat algoritma ciphering (A5). Algoritma enkripsi (A3, A5, A8) digunakan juga pada jaringan GSM. Authetifikasi Center (AUC), yang merupakan bagian dari Operation and Maintenance Subsystem (OMS) dari jaringan GSM terdiri database identifikasi dan informasi autentifikasi untuk pengguna. Informasi ini terdiri dari IMSI, Temporary Mobile Subscriber Identity (TMSI), identita lokasi area (LAI) dan kuncu autentifikasi pelanggan (Ki) untuk setiap user. Untuk menjalankan fungsi keamanan dan autentifikasi diperlukan tiga element tersebut (SIM, handset dan jaringan GSM). Distribusi dari faktor keamanan dan algoritma enkripsi ini menghasilkan faktor keamanan yang lebih untuk menjaga privasi dari pengguna SMS banking ini.



Gambar 8. Distribusi Fitur Keamanan SMS Banking

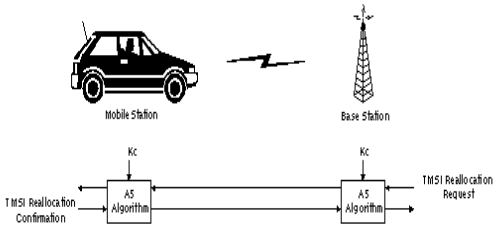
Langkah-langkah keamanan yang dilakukan pada SMS banking adalah sebagai berikut ;

1. Autentifikasi
   Jaringan GSM akan memeriksa identitas pelanggan dengan menggunakan mekanisme respon. Nomor random (RAND) akan dikirmkan ke MS. Kemudian MS akan mengirimkan respoon berdasarkan enkripsi dari RAND dengan algoritma A3 dan kunci autentifikasi pelanggan. Selama menerima SRES dari pelanggan, jaringan GSM akan mengulan perhitungan untuk melakukan verifikasi identitas dari pelanggan. Jika SRES sesuai dengan nilai yang dihitung MS telah berhasil diautentifikasi dan akan dilanjutkan. Jika tidak sesuai maka koneksi akan diputus. Berikut ini ilustrasi yang menggambarkan proses autentifikasi :



Gambar 9. Mekanisme Autentifikasi jaringan GSM

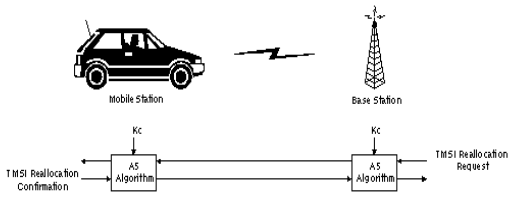
2. Signaling data
   SIM mengandung algoritma A8 yang akan menghasilkan ciphering key (Kc). Ciphering key didapatkan dengan menggunakan RAND yang digunakan untuk proses autentifikasi dengan menggabungkan dengan kunci autentifikasi pelanggan (Ki). Ciphering key digunakan untuk enkripsi dan dekripsi antara MS dan BS. Keamanan dapat ditingkatkan ketika ciphering key yang digunakan berubah-ubah pada tiap langkahnya.
   Enkripsi data antara MS dan network dilakukan dengan menggunakan algoritma A5. Komunikasi yang terenkripsi diawali dengan permintaan ciphering mode dari jaringan GSM. Selama menerima perintah ini, MS akan melakukan enkripsi dan dekripsi data menggunakan algoritma A5 dan ciphering key.



Gambar 10. Mekanisme inisiasi ciphering mode

3. Pengecekan Identitas
   Untuk memastikan kerahasiaan identitas, Temporary Mobile Subscriber Identity (TMSI) akan digunakan. TMSI akan dikirimkan ke MS setelah proses autentifikasi dan dekripsi dilakukan. MS akan

merespon dengan mengkonfirmasi penangkapan TMSI. TMSI valid pada area yang telah diperkirakan. Untuk komunikasi di luar area, LAI (Location Area Identification) akan ditambahkan ke TMSI.



Gambar 11. Metode realokasi TMSK

B. Enkripsi pada SMS Banking

SMS banking menggunakan beberapa langkah untuk meningkatkan faktor keamanannya salah satunya adalah dengan mengenkripsi data yang ada. Enkripsi ini biasanya dilakukan pada saat transmisi yang dilakukan SMS dari pengguna ke base station. Selain itu biasanya pihak bank juga melakukan enkripsi data pada saat pengiriman dai service provider. Enkripsi dilakukan dengan menggunakan algoritma kriptografi modern karena enkripsi pesan dilakukan dalam bentuk bit. Hal ini dilakukan agar keamanan pesan lebih tinggi. Algoritma yang umum digunakan adalah A8 dan A5. Algoritma A8 digunakan untuk membuat kunci cipher 64 bit. Kunci yang dihasilkan oleh algoritma ini akan digunakan dalam algoritma A5 untuk mengenkripsi pesan yang dikirimkan pelanggan ke base station.

Algoritma enkripsi ini sangat berguna untuk meningkatkan faktor keamanan pada SMS banking. Data dari pengguna yang rawan disadap akan dienkripsi menjai bentuk yang sulit dipecahkan karena menggunakan kombinasi algoritma kriptografi. Jika data sms dapat disadap maka proses enkripsi inilah yang akan menjadi pelindung kedua data. Data yang disadap akan terlihat sebagai simbol-simbol unik yang tidak dapat dipecahkan dengan metode tradisional.

IV. KESIMPULAN

Berdasarkan hasil analisis dapat diambil beberapa kesimpulan :

1. Layanan SMS banking masih rawan dengan kasus kejahatan, terutama penyadapan
2. Algorima kriptografi modern A5 dan A8 digunakan untuk proses enkripsi pada layanan SMS banking
3. Algoritma kriptografi modern dapat meningkatkan faktor keamanan pada layanan SMS banking

REFERENCES

[1] Le Bodic, Gwenae¨l. 2005. Mobile Messaging Technology and Services. West Sussex, England: John Wiley & Sons Ltd
[2] CME 20 SYSTEM SURVEY TRAINING DOCUMENT. 1996. Ericsson Radio Systems AB.
[3] http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html
[4] http://palisade.plynt.com/issues/2005Sep/sms-banking/

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 20 Maret 2011

Biyan Satyanegara / 13508057