Secure SMS Banking Menggunakan Teknik Enkripsi Kompresi Hybrid

Ananti Selaras Sunny (13507009)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if17009@students.if.itb.ac.id

***Abstrak*—Perkembangan teknologi yang semakin cepat, semakin memudahkan orang dalam mengakses berbagai informasi. Ada berbagai macam cara mengakses informasi salah satunya dengan menggunakan teknologi SMS (Short Message Service). Hanya saja untuk dalam perjalanan informasinya melalui teknologi SMS memiliki kelemahan dalam hal keamanan data yang dikirimkan, akan tetapi SMS merupakan teknologi yang mudah dan banyak yang meminatinya. Berhubungan dengan teknologi banking yang sedang berkembang, sekarang pihak pengembang melirik teknologi perbankan dengan memanfaatkan teknologi SMS. Belakangan ini sudah semakin banyak bank yang menerapkan teknologi SMS ini untuk urusan perbankan mereka, biasa disebut SMS Banking. SMS Banking memudahkan konsumen dalam melakukan transaksi perbankan, sehingga semakin banyak pengembang SMS Banking ini. Pihak pengembang seharusnya bertanggung jawab dalam mengelola keamanan data SMS Banking, karena protokol GSM secara opsional melakukan enkripsi data yang melewatinya. Bila dilakukan enkripsi pun, algoritmanya tidak begitu kuat, masih tergolong lemah. Maka untuk meningkatkan keamanan data yang dikirimkan seharusnya melalui tahap enkripsi terlebih dahulu.**

***Keyword*—SMS Banking, Protokol GSM, keamanan data, enkripsi, perbankan.**

I. PENDAHULUAN

Pada zaman sekarang ini, teknologi merupakan kebutuhan utama setiap orang. Salah satu teknologi yang tidak bisa terlepas dari genggaman setiap orang adalah teknologi telekomunikasi, secara khususnya adalah teknologi ponsel. Hampir semua orang memiliki ponsel, dari yang tua sampai muda. Adanya ponsel ini, dapat mempercepat dan mempermudah penyaluran informasi. Salah satu teknologi ponsel yang banyak diminati dan digunakan adalah SMS (Short Message Service).

SMS (Short Message Service) adalah komunikasi standar dalam komunikasi melalui GSM. SMS dapat dikirim dan diterima secara simultan, data yang dikirimkan dapat berupa teks. SMS merupakan aplikasi yang paling banyak digunakan di dunia, dengan pengguna aktif sebesar 2,4 milyar atau sekitar 74% dari pengguna ponsel di dunia. Hal ini disebabkan layanan SMS merupakan layang yang mudah digunakan, cepat, efisien, dan murah.

Belakangan ini, teknologi SMS digunakan dalam dunia perbankan. Secara fungsionalitasnya seperti transaksi pada umumnya, misalnya melihat saldo atau transfer uang ke rekening lain. SMS dipilih karena semua provider dan hampir semua jenis ponsel memiliki fungsionalistas ini dan SMS dinilai lebih praktis, tidak perlu koneksi internet sama sekali, serta secara tarif juga tergolong murah. Maka dibuatlah fasilitas SMS Banking untuk melakukan transaksi perbankan melalui SMS. Setelah dirilisnya fasilitas SMS Banking ini, semakin banyak pengguna yang menggunakannya, sehingga hal ini membuat perkembangan SMS Banking semakin pesat, banyak bank-bank di Indonesia yang sudah memiliki fasilitas ini.

Permasalahan dalam SMS Banking ini adalah perlu dipertanyakannya tentang keamanan dari SMS Banking. Karena data-data yang dikirimkan bersifat rahasia, harus ditingkatkan keamanannya. Data-data yang dipertukarkan adalah nomor rekening dan transaksi pengguna, yang sifatnya sangat privasi. Maka data yang dipertukarkan sebaiknya dilakukan enkripsi untuk meningkatkan keamanannya.

II. SMS (SHORT MESSAGE SERVICE)

Gambar 1 Skema SMS

Pesan dikirim dengan SMS-MT (melalui telepon atau aplikasi perangkat lunak) dan SMS-MO (melaui ponsel) panjangnya selalu dibatasi pada 160 karakter (untuk satu satuan SMS). Hal ini erat kaitannya dengan awal pembutan sms yang memanfaatkan ruang sisa pada jalur sinyal GSM seperti yang telah diceritakan sebelumnya. Sisa ruang itu dibatasi panjangnya tepat 140 octets atau 1120 bits. Kemudian pesan singkat dapat di-enkoding dengan berbagai standar abjad. Sebagai default standarnya adalah dengan 7 bit alfabet, yang lain dengan 8 bit alfabet atau 16 bit UTF-16 alfabet.

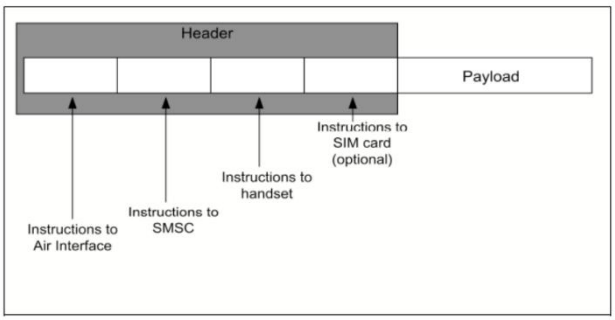
Bila menggunakan 7 bit alfabet (7 bit alfabet merupakan standar untuk karakter huruf inggris,termasuk yang dipakai Indonesia) maka panjang karakter maksimal per sms adalah 160 karakter (termasuk spasi). Sedangkan untuk 8 bit maksimal 140 karakter dan 16 bit alfabet maksimal 70 karakter.

Karakter-karakter khusus seperti huruf Arab, Jepang, Korea dll biasanya menggunakan tipe 16 bit karakter ini di-encoding dengan 16 bit dan merupakan karakter Unicode UCS2. Selain teks pesan dengan tipe bit karakter di atas, sms juga dapat membawa data biner seperti nada dering, gambar, logo operator, kartu nama (VChards), WAP konfigurasi yang memanfaatkan sisa 1120 bits ini.

Karena keterbatan panjang SMS ini maka kemudian muncullah Long SMS. Long sms akan mengirimkan beberapa pesan dipecah-pecah yang dimulai dengan User data Header berisi informasi segmentasi. Kemudian mengirimkannya masing-masing sebagai satu pesan SMS. Kemudian setelah sampai di ponsel tujuan, ponsel penerima akan merangkai kembali beberapa pesan tersebut menjadi satu kesatuan pesan lagi, inilah yang disebut long SMS.

Pada perkembangannya untuk menutupi kekurangan pada SMS dikembangkan EMS (Enhanced Mesagging Service) yang dapat berisi gambar bergerak (animasi) atau melodi.

SMS terdiri dari beberapa metadata, yaitu informasi tentang pengguna (servis center kontak, kontak pengirim), informasi tentang protokol (protocol identifier, data coding scheme), dan waktu.



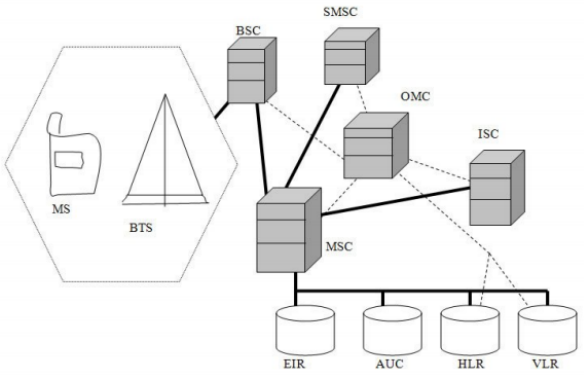
Gambar 2 Struktur SMS

Dari gambar diatas dapat dilihat bahwa SMS terdiri dari dua elemen utama, yaitu header and user data (the message body).

SMS dikirim dan diterima berupa plainteks biasa dan privasi SMS tidak bisa dijamin, tidak hanya saat dikirim tetapi juga SMS yang disimpan pada ponsel tersebut. Isi dari SMS terlihat di operator jaringan. Kebutuhan untuk aktif SMS yang berdasarkan layanannya hanya bisa dipuaskan ketika ada teknologi end-to-end security.

III. TEKNOLOGI GSM

GSM terdiri dari bermacam-macam komponen yang digambarkan dengan keterhubungan garis yang solid dan putus-putus. Sinyal komunikasi ditransmisikan dari MS (Mobile Station) dan diterima oleh BTS (Base Transceiver Station). Fungsi dari BTS adalah untuk menerima dan mentransmisikan sinyal menuju dan dari MS. BTS juga bertanggung jawab untuk mentranslasikan sinyal dalam bentuk format digital dan mentransferkannya pada BSC (Base Station Controller). BSC menyalurkan sinyal yang diterimanya ke MSC (Mobile Switching Center). MSC lalu menanyai Home dan Visitor Location Registers di database untuk menyimpan informasi lokasi dan tujuan MS. Dalam proses tersebut, sinyal yang diterima merupakan SMS lalu dirutekan ke SMSC untuk dikirimkan pada tujuan yang dibutuhkan. Lalu, SMSC menyimpan salinan dari SMS yang dikirimkan.



Gambar 3 Arsitektur GSM

Keamanan dari GSM juga harus diperhatikan. Untuk melakukan perlindungan terhadap jaringan operator dan pengguna GSM menyediakan implementasi dari banyak fasilitas keamanan. Fitur yang diambil dari perpektif pengguna, antara lain kemanan identitas secara rahasia, autentifikasi identitias, data pengguna yang rahasia.

Protokol GSM dapat dienkripsi atau tidak dienkripsi tergantung kebikakan yang ada. Dalam enkripsi protokol GSM menggunakan algoritma A5, jenisnya terdapat dua, yaitu A5/1 dan A5/2. Algoritma A5 dinilai lemah karena sudah berhasil dibobol oleh kriptanalis. Jika algoritma enkripsinya saja sudah bisa dibobol maka secara otomatis keamanan protokol jaringan GSM.

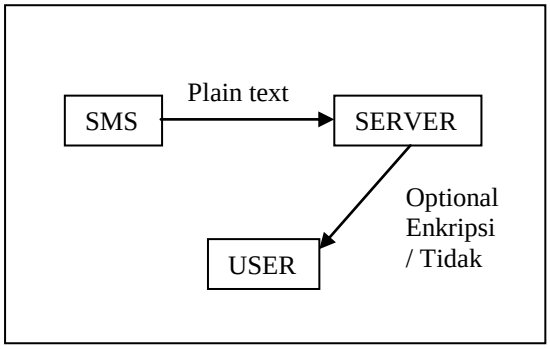
Untuk autentifikasi algoritma biasanya menggunakan autentifikasi melalui luar sistem akan tetapi algoritma autentifikasi sudah bisa dipecahkan dan berhasil mengambil kunci dan kontak .

IV. SMS BANKING

Beberapa bank sudah menerapkan SMS Banking menjadi salah satu fiturnya. Penggunan cukup mengetikkan kode tertentu untuk melakukan transaksi dan dikirimkan melalui SMS. Saat SMS dikirimkan, pesan tidaklah dienkripsi. Lalu SMS tersebut diterima oleh server, seperti SMS Gateway, kemudian oleh server diambil data yang dimaksudkan. Saat mencari dan mengambil data yang dibutuhkan data dienkripsi. Saat pengiriman data yang dimintai oleh pengguna dapat dienkripsi terlebih dahulu atau tidak saat dikirimkan kembali, hal ini bergantung dengan kesepakatan antara

developer dan provider.

Untuk metode enkripsi yang digunakan juga bisa apa saja tergantung kebutuhan dan permintaan user (client). Jika melakukan enkripsi saat pengirimin data ke pengguna maka akan membutuhkan biaya yang lebih



Gambar 4 Skema sederhana

Analisis keamanan pada SMS Banking,

1. Plainteks SMS dikirimkan melalui protokol GSM yang hanya dienkripsi menggunakan algoritma A5, akan tetapi ada juga protokol GSM yang tidak melalui proses enkripsi terlebih dulu, sehingga semakin rawan saat pertukaran data terjadi. Algoritma A5 bukan merupakan enkripsi yang aman, karena peneliti telah membuktikan bahwa algoritma tersebut dapat ditembus dan tidak tahan terhadap serangan.
2. SMS yang menunggu untuk dikirim disimpan di store di dalam penyedia layanan yang berupa plainteks. Meskipun setelah pesan terkirim, penyedia layanan menyimpan semua pesan. Jika isi pesan tidak dienkripsi maka orang lain yang mendapatkan akses ke provider bisa melihat data yang bersifat privasi milik pengguna.
3. USSD banking. Verifikasi tergantung hanya pada nomor pengirim , jika SIM card hilang atau diduplikasi, maka penyerang dapat menggunakan akun korban yang melakukan transaksi. Pesan USSD yang dikirimkan ke server bank hanya dienkripsi antara mobile station dan base receiver station. Pesan adalah plainteks yang ada di dalam jaringan operator telepon.
4. Pin authentifikasi. Bank nasional pertama menggunakan USSD untuk memperbolehkan konsumen mereka mengirimkan autentifikasi pin. Penyedia layanan dapat membaca Pin karena dikirimkan berupa plainteks.
5. Beberapa SMS Banking menggunakan WIG dengan SIM menu sebagai aplikasi. Jika aplikasi ini dimuat ke dalam SIM card maka membuat aplikasi mobile banking SIM card dependent. Jika SIM card hilang, maka keamanannya terancam.

Maka untuk meningkatkan keamanan dalam SMS Banking diperlukan peningkatan enkripsinya atau membuat desain baru dalam pengiriman SMS tersebut yang berupa plainteks.

V. ALGORITMA AES

AES adalah singkatan dari Advance Encryption Standard adalah enkripsi dengan enkripsi kunci simetri, standarnya diadopsi oleh pemerintah Amerika. Jenis algoritma AES ada tiga, yaitu AES-128, AES-192 dan AES-256, yang merupakan adopsi dari kumpulan algoritma yang lebih besar yang aslinya dibuat oleh Rijndael. Setiap cipher memiliki 128-bit block size, dengan kunci berukuran of 128, 192 and 256 bit. AES cipher memliki dan sudah dianalisis secara ekstensif dan digunakan di seluruh dunia.

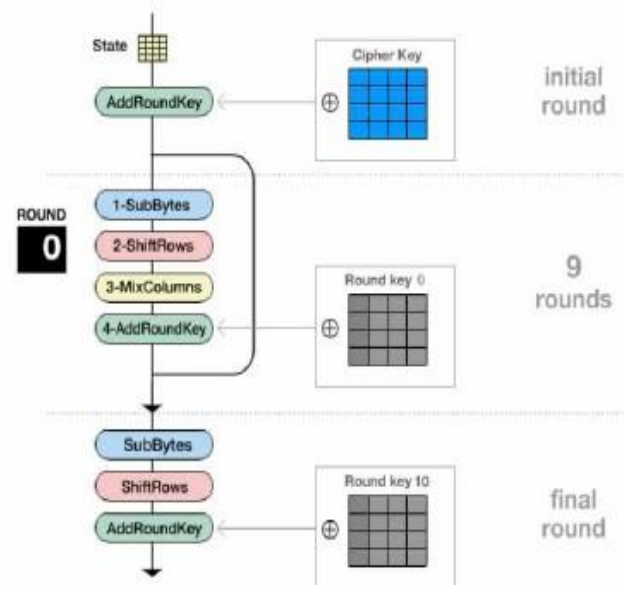
Rijndael (AES) menggunakan blok input atau blok data dengan ukuran 128 bit, panjang kunci yang digunakan adalah 128, 192, dan 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah round atau putaran pada algoritma Rijndael (AES). Di bawah ini adalah tabel perbedaan kunci algoritma tersebut.

	Jumlah Key (Nk)	Besar Block (Nb)	Jumlah Round (Nr)
AES – 128	4	4	10
AES – 192	6	4	12
AES – 256	8	4	14

Tabel 1 Perbandingan jumlah round dan key

Secara garis besar proses enkripsi data pada AES adalah sebagai berikut: Parameter algoritma AES terdiri dari tiga bagian :

1. *Plaintext* : *array* berukuran 16 *byte* merupakan data masukan
2. *Ciphertext* : *array* berukuran 16 *byte* merupakan hasil *enkripsi*
3. *Cipher Key* : *array* berukuran 16 *byte* merupakan kunci *enkripsi*

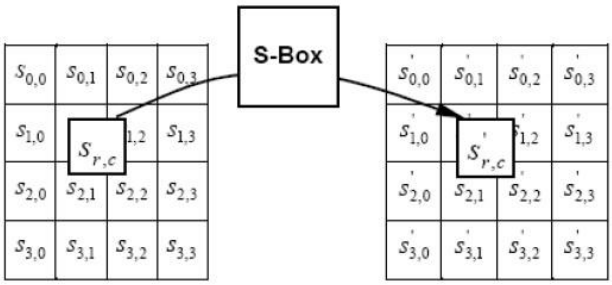


Gambar 5 Blok Diagram Proses Enkripsi dan Dekripsi AES

Dengan menggunakan ukuran 16 *byte* maka blok data dan kunci yang berukuran 128 bit dapat disimpan di dalam ketiga *array* tersebut (128 = 16 x 8). Kalkulasi *plaintext* menjadi *ciphertext* status dari data disimpan di dalam *array of bytes* dua dimensi yang dinamakan *state* Untuk ukuran blok data 128 bit ukuran *state* adalah 4 x 4. Elemen *array state* diacu sebagai S[r,c] dengan 0 ≤ r C 4 dan 0 ≤ c V Nb (Nb adalah panjang blok dibagi 32. Pada AES-128 Nb = 128/ 32 = 4).

Transformasi *SubBytes*

Transformasi *SubBytes* merupakan substitusi *byte* non-linear yang beroperasi pada setiap *state bytes*secara tersendiri. Pada proses ini setiap *byte* dari *array state* disubstitusikan menggunakan tabel substitusi (*S-Box*).

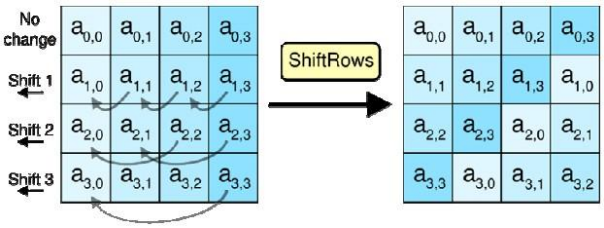


Gambar 6 Transformasi SubBytes

Transformasi dilakukan pada masing-masing *byte* pada *array state*. Nilai pengganti ditentukan dari nilai kolom c dan baris r *S-Box* dengan merunut perpotongan dari nilai c dan r dari *array state*.

Transformasi *ShiftRows*

Transformasi *ShiftRows* melakukan pergeseran secara *wrapping* pada 3 baris terakhir dari *array state*. Baris pertama dari *array state* tidak mengalami pergeseran, sesuai dengan ketentuan pergesaran yaitu berdasarkan nilai baris r (r = 0 tidak digeser, r = 1 digeser sejauh 1 byte, r = n digeser sejauh n*byte*).



Gambar 7 Transformasi ShiftRows

Transformasi MixColumns

Transformasi *MixColumns* melakukan proses perkalian nilai byte pada setiap kolom dari *array state*dengan polinom a(x)mod(xˆ4 +1). Setiap kolom dianggap sebagai polinom 4-suku pada GF(2ˆ8), dengan rumus :

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$

Transformasi ini dinyatakan dalam perkalian matriks,

$$s'(x) = a(x) \otimes s(x)$$

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

Transformasi *AddRoundKey*

Pada proses transformasi ini dilakukan operasi XOR sederhana terhadap *round key* dengan *array state*.*Round key* diperoleh dari *cipher key* sesuai dengan nilai *key* masing–asing *round*. Hasil dari operasi ini disimpan di dalam *array state*.

Camellia Encryption

Camellia encryption merupakan jenis algoritma block chiper yang dikembangkan di Jepang oleh perusahaan NTT pada tahun 2000. Algoritma ini masih tergolong baru tetapi telah masuk ke dalam kandidat AES.

Sebelum mempelajari proses kriptografi pada algoritma Camellia terlebih dahulu harus mengetahui simbol-simbol yang tedapat dalam proses.

$x \oplus y$	Operasi XOR antara elemen x dan y
$x \parallel y$	Operasi CONCAT antara elemen x dan y
$x <<< n$	Operasi ROTATE LEFT elemen x sebanyak n
$x \cap y$	Operasi AND antara elemen x dan y
$x \cap y$	Operasi OR antara elemen x dan y
$!x$	Operasi NOT dari elemen x

Tabel 2Daftar Simbol pada Proses Algoritma Camellia

Dalam melakukan enkripsi Camellia terdapat proses yang membutuhkan *key* untuk melindungi dokumen dan menggunakan S-box untuk meningkatkan keamanan data.Dibawah ini adalah komponen–komponen penyusun pada proses enkripsi dan dekripsi algoritma Camellia.

a. F-Function

F-function didefinisikan sebagai berikut :

$$\mathbf{F : L \times L \rightarrow L}$$

$$\mathbf{(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = P(S(X_{(64)} \oplus k_{(64)}),}$$

b. P-Function

b. P- Function

P-function adalah bagian dari F-function yang didefinisikan sebagai berikut :

$$\mathbf{P : L \rightarrow L}$$

$$\mathbf{Z_{1(8)} \parallel Z_{2(8)} \parallel Z_{3(8)} \parallel Z_{4(8)} \parallel Z_{5(8)} \parallel Z_{6(8)} \parallel Z_{7(8)} \parallel Z_{8(8)} \rightarrow Z'_{1(8)} \parallel Z'_{2(8)} \parallel Z'_{3(8)} \parallel Z'_{4(8)} \parallel Z'_{5(8)} \parallel Z'_{6(8)} \parallel Z'_{7(8)} \parallel Z'_{8(8)}}$$

Syarat:

$$z'_1 = z_1 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8,$$
$$z'_2 = z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_7 \oplus z_8,$$
$$z'_3 = z_1 \oplus z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_8,$$
$$z'_4 = z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7,$$
$$z'_5 = z_1 \oplus z_2 \oplus z_6 \oplus z_7 \oplus z_8,$$
$$z'_6 = z_2 \oplus z_3 \oplus z_5 \oplus z_7 \oplus z_8,$$
$$z'_7 = z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_8,$$
$$z'_8 = z_1 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7.$$

c. S-Function

$S : L \rightarrow L$

$I_{1(8)} \| I_{2(8)} \| I_{3(8)} \| I_{4(8)} \| I_{5(8)} \| I_{6(8)} \| I_{7(8)} \| I_{8(8)} \rightarrow I'_{1(8)} \| I'_{2(8)} \| I'_{3(8)} \| I'_{4(8)} \| I'_{5(8)} \| I'_{6(8)} \| I'_{7(8)} \| I'_{8(8)}$

Syarat:

$$I'_{1(8)} = S_1(I_{1(8)})$$
$$I'_{2(8)} = S_1(I_{2(8)})$$
$$I'_{3(8)} = S_1(I_{3(8)})$$
$$I'_{4(8)} = S_1(I_{4(8)})$$
$$I'_{5(8)} = S_1(I_{5(8)})$$
$$I'_{6(8)} = S_1(I_{6(8)})$$
$$I'_{7(8)} = S_1(I_{7(8)})$$
$$I'_{8(8)} = S_1(I_{8(8)})$$

d. FL-Function

FL-function didefinisikan sebagai berikut :

$$\mathbf{FL : L \times L \rightarrow L}$$
$$\mathbf{(X_{L(32)} \| X_{R(32)}, kl_{R(32)} \| kl_{R(32)}) \rightarrow Y_{L(32)} \| Y_{R(32)},}$$

Dimana:

$$Y_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) <<1) \oplus X_{R(32)},$$
$$Y_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus X_{L(32)},$$

e. FLˆ-1 Function (FLˆ-1)

FLˆ-1-function didefinisikan sebagai berikut :

$$\mathbf{FL^{-1} : L \times L \rightarrow L}$$
$$\mathbf{(Y_{L(32)} \| Y_{R(32)}, kl_{L(32)} \| kl_{R(32)}) \rightarrow X_{L(32)} \| X_{R(32)},}$$

Syarat :

$$X_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus Y_{L(32)},$$
$$X_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) <<1) \oplus Y_{R(32)},$$

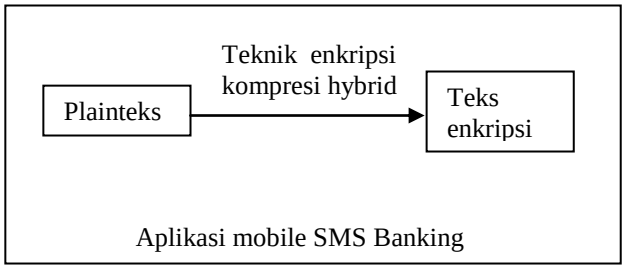
Syarat :

$$X_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus Y_{L(32)},$$
$$X_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) <<1) \oplus Y_{R(32)},$$

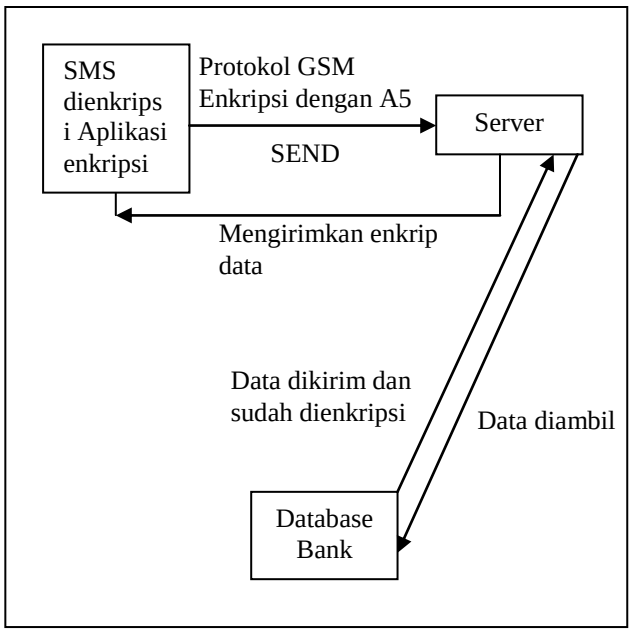
VI. RANCANGAN SMS BANKING

Seperti sebelumnya yang sudah dijelaskan. Pengiriman data pengguna yang menggunakan SMS Banking hanya berupa plainteks biasa, sehingga akan mudah disadap oleh orang lain. Lagipula protokol GSM bisa saja dienkripsi atau tidak dengan menggunakan algoritma A5. Padahal algoritma ini sudah pernah berhasil dibobol oleh kriptanalis dan dinyatakan tidak aman. Maka pada SMS Banking perlu dibuat enkripsi berlapis supaya meskipun protokol GSM dapat ditembus, tetapi pesan tetap tidak dapat dimengerti orang lain, karena data pesan sebelumnya sudah dienkripsi.

Jika sebelumnya pengiriman SMS Banking hanya berupa plainteks biasa, maka saya akan mengajukan desain SMS Banking.



Gambar 8 Enkripsi menggunakan aplikasi



Gambar 9 Skema pengiriman dan penerimaan

Seperti yang dijelaskan sebelumnya, agar data yang dikirimkan tetap terjaga keamanannya maka data dienkripsi terlebih dahulu. Proses utama yang dilakukan disini ada dua, yaitu kompresi pesan dan enkripsi pesan. Kompresi pesan adalah proses encoding infromasi SMS menggunakan bit yang lebih sedikit. Tujuannya adalah untuk mengurangi konsumsi data dan mengurangi panjang SMS. Setelah dilakukan kompresi maka plainteks siap melalui tahap enkripsi.

Untuk tahap selanjutnya adalah enkripsi data. Enkripsi dapat dilakukan dengan algoritma yang apapun dengan melihat tingkat keamanan algoritma tersebut. Dalam konteks ini, digunakan enkripsi menggunakan algoritma AES (Advanced Encryption Standard). AES dipilih karena sejauh ini algoritma enkripsi yang memiliki performansi yang paling bagus adalah AES.

Setelah plainteks yang berisi transaksi banking itu

melalui tahap enkripsi, maka data enkripsi siap dikirimkan melalui jaringan GSM. Jaringan GSM secara opsional mengenkripsi data menggunakan algoritma A5. Secara keamanan algoritma S5 tidak aman, tetapi dengan data yang dikirimkan sudah dienkripsi terlebih dahulu membuat pengguna tidak perlu khawatir data transaksi banking tersebut bocor.

Lalu sampailah data yang terenkripsi itu dan diterima oleh server. Server ini berfungsi mendekripsikan data tadi menjadi plainteks, yang kemudian akan dikenali sebagai perintah transaksi. Setelah didapatkan plainteks maka diambillah data transaksi yang dimaksud dari server bank. Lalu setelah itu data yang diminta oleh pengguna dikirimakan ke server, sebelumnya data sudah dienkripsi terlebih dahulu. Setelah itu, sampai di server didekripsi dan siap dienkripsi kembali untuk dikirimkan melalui protokol GSM.

Sampai pada pengguna data berupa enkripsi yang kemudian akan didekripsi oleh aplikasi SMS Banking tersebut. Dan data yang dimaksudkan oleh pengguna secara aman terkirimkan.

Walaupun agak merepotkan karena harus membuat aplikasi SMS Banking untuk enkripsi dan harus berulang-ulang enkripsi-dekripsi, hal ini bertujuan untuk meningkatkan keamanan dalam transaksi perbankan yang melewati protokol GSM.

SMS Banking yang sekarang ada tidak mengirimkan data melalui tahap enkripsi terlebih dahulu. Enkripsi data hanya dilakukan saat mengambil data pada server bank dan data dikirimkan ke konsumen dalam bentuk plainteks, serta saat melewati protokol GSM terkadang tidak dienkripsi. Hal ini sangat berbahaya karena data transaksi bisa bocor.

VII. PENINGKATAN KEAMANAN SMS BANKING

Setelah sebelumnya dibahas tentang skema yang ditawarkan untuk meningkatkan keamanan pada SMS Banking, dengan desain tersebut diharapkan menjadi kajian lebih lanjut.

Desain untuk meningkatkan keamanan dalam bertansaksi menggunakan SMS Banking ini dapat dirujuk menjadi beberapa poin, yaitu:

- Pada skema umumnya, pesan yang dikirimkan dari pengguna masih berupa plainteks, hal itu membahayakan maka perlu mengenkripsi pesan agar lebih aman ketika melewati protokol GSM.
- Dilakukan kompresi data agar mengurangi konsumsi data.
- Algoritma enkripsi yang digunakan adalah AES, algoritma ini dinilai paling aman sejauh ini dan dapat menangani kompresi data.
- Untuk kompresi dan enkripsi ini dilakukan dalam aplikasi mobile.
- Pada skema umumnya pengiriman data yang diminta oleh pengguna, biasanya tidak dienkripsi, yang dienkripsi adalah protokol GSM-nya. Sedangkan terkadang ada juga yang tidak dienkripsi protokol GSM-nya. Data yang dikirimkan tersebut sudah dienkripsi terlebih dahulu agar tidak bocor ketika melewati protokol GSM.

VIII. KESIMPULAN

Kesimpulan yang bisa diambil dari makalah ini, yaitu:

- SMS Banking biasa masih kurang aman, karena mengirimkan data dalam bentuk plainteks.
- Protokol GSM terkadang dienkripsi dan kadang tidak, jika dienkripsi maka menggunakan algoritma A5, yang dinyatakan kurang aman.
- Kompresi data yang akan dikirim bertujuan untuk mengurangin konsumsi data.
- Algoritma AES merupakan algoritma teraman sejauh ini dan dapat menangani kompresi data.
- Mengenkripsi data yang dikirim dan diterima maka akan meningkatkan kerahasiaan informasi.
- Solusi enkripsi data yang dikirim dan dekripsi data yang diterima menggunakan aplikasi mobile.

REFERENSI

[1] Mobile Banking in Developing Country Emmanuel, Abunyang.2007

[2] Komunikasi melalui SMS http://candrapamungkas.web.ugm.ac.id/?p=85 tanggal akses 22 Maret 2011

[3] Secure SMS Banking http://people.cs.uct.ac.za/~kumoyo/chnmin016/project/resources/Secure_SMS_Banking.pdf tanggal akses 22 Maret 2011

[4] Advance Encryption Standard http://en.wikipedia.org/wiki/Advanced_Encryption_Standard tanggal akses 23 Maret 2011

[5] Advance Encryption Standard http://www.ittelkom.ac.id/library

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, 23 Maret 2011

Ananti Selaras Sunny (13507009)