Serangan pada Algoritma A3,A5,dan A8 di Jaringan GSM dan Penerapan Elliptic Curve Chryptography Untuk Mengatasinya

Ardian Franindo-NIM:13504106
Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if114106@students.if.itb.ac.id

Abstract
Sistem jaringan GSM (Global System for Mobile) merupakan jaringan seluler yang paling banyak digunakan masyarakat Indonesia. Untuk menjamin aspek keamanan, Kerahasiaan data dan sinyal dilakukan dengan melakukan enkripsi dengan algoritma tertentu, pada umumnya pada jaringan GSM digunakan algoritma A3, A5 dan A8
Meskipun jaringan GSM sudah dilengkapi dengan sistem pengamanan seperti tersebut diatas, tetapi jaringan GSM masih rentan terhadap serangan kriptanalis terhadap algoritma, pengkloningan SIM card, serta ekstraksi kunci dari kartu SIM. Pada sistem keamanan jaringan GSM, ditemukan beberapa kelemahan yang bisa merugikan kepentingan-kepentingan pelanggan dan jaringan. Kelemahan tersebut terutama terjadi pada pengamanan data di luar link radio.
Pengkombinasian metoda kriptografi ECC (Elliptic Curve Cryptography) dengan algoritma A3, A8, dan A5 untuk mendapatkan kualitas keamanan yang lebih baik. Pengkombinasian metoda ECC diterapkan dalam layananan sistem keamanan jaringan GSM, terutama pada proses autentikasi dan pengamanan identitas pelanggan. Parameter yang digunakan sebagai perbandingan dalam analisis adalah skema sistem keamanan dan pengujian avalanche effect.

***Kata Kunci**: Algoritma A3,A5, dan A8, Serangan pada jaringan GSM, Elliptic Curve Chryptography*

1. PENDAHULUAN

GSM (Global System for Mobile) adalah jaringan selular yang paling banyak digunakan saat ini. GSM adalah telepon selular digital pertama setelah era analog. Masalah dari sistem analog adalah kemungkinan untuk melakukan pengkloningan telepon untuk melakukan panggilan telepon terhadap orang lain dengan maksud penipuan, selain itu sistem analog juga berpotensi dapat melakukan penyadapan (*eavesdrop*) panggilan telepon. Jaringan GSM bertujuan untuk memperbaiki masalah tersebut dengan mengimplementasikan autentifikasi yang kuat antara telepon selular dan MSC (*mobile service switch center*), mengimplementasikan enkripsi data yang kuat pada transmisi udara antara MS dan BTS.

GSM adalah standar eropa untuk komunikasi selular digital. GSM dideklarasikan pada tahun 1982 pada European Conference of Post and Telecommunication Administrations (CEPT). Lebih lanjut, sejarah GSM sebagai standar komunikasi digital disepakati dalam GSM MoU pada tahun 1987, dimana 18 negara sepakat untuk mengimplementasikan jaringan selular yang berbasis GSM. Pada tahun 1991 Jaringan GSM pertama kali muncul. [3]

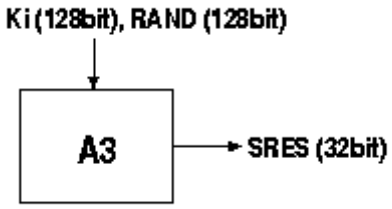
Jaringan GSM saat ini digunakan algoritma A3, A8, dan A5 dalam sistem pengamanannya. Algoritma A3 dan A8 digunakan dalam proses autentikasi, yaitu proses pengenalan identitas pelanggan, yang terjadi pada MS (*Mobile Station*) dan AUC (*Authentication Centre*). Sedangkan algoritma A5 digunakan dalam proses pengiriman informasi pada link radio antara MS dengan BTS (*Base Transceiver Station*). Namun pada sistem pengamanan dengan menggunakan algoritma ini ditemukan kelemahan-kelemahan yang memungkinkan terjadinya penyadapan data ataupun penipuan identitas pelanggan.digunakan pula jaringan feistel atau dan chiper berulang. [5]

Untuk mengatasi kelemahan-kelemahan itu, pada tugas akhir ini ditawarkan penggunaan ECC (Elliptic Curve Crytography) untuk dikombinasikan dengan algoritma sistem keamanan jaringan GSM. Pengkombinasian ini diharapkan bisa menghasilkan kualitas sistem keamanan yang lebih baik. [2]

2. ALGORITMA JARINGAN GSM

2.1 Algoritma A3

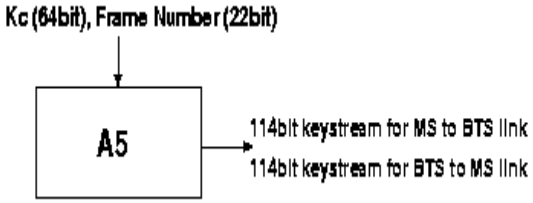
Algoritma A3 adalah algoritma autentifikasi dalam model keamanan GSM. Fungsi A3 yaitu untuk membangkitkan response yang lebih dikenal dengan SRES sebagai jawaban dari random challenge yang dikenal dengan RAND.
Algoritma A3 mendapatkan nilai RAND dari MSC dan kemudian dengan kunci Ki dari SIM membangkitkan 32 bit sebagai keluaran yang mana disebut response SRES. Baik RAND maupun Ki adalah nilai rahasia sepanjang 128 bit.



Gambar 1 Sign Response (SRES) dihitung dengan melihat nilai RAND dan Ki

2.2. Algoritma A5

Algoritma A5 adalah cipher aliran yang digunakan untuk mengenkripsi pesan dalam transmisi udara. Cipher aliran ini diinisialisasi setiap frame dikirim. Cipher aliran ini diinisialisasi dengan kunci sesi, Kc, dan jumlah frame yang akan dienkripsi. Kunci sesi yang sama digunakann sepanjang panggilan berlangsung, tetapi 22 bit nomor *frame* berubah selama proses berlangsung, kemudian membangkitkan *keystream* yang unik untuk setiap *frame*.



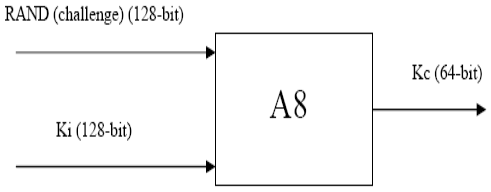
Gambar 2, Pembakitan Keystream

Kunci yang digunakan dalam algoritma ini adalah 64 bit Kc, ditambah inputan berupa nomer *frame* TDMA dalam suatu multiframe. Output yang dihasilkan berupa sepasang 114 bit *codeword* (S1 dan S2) untuk arah *downlink* dan *uplink*. Selanjutnya masing-masing *codeword* di-XOR dengan 114 bit *plain text* untuk menghasilkan 114 bit *chipertext* yang akan dikirimkan

2.3. Algoritma A8

Algoritma A8 adalah algoritma yang berfungsi untuk membangkitkan kunci sesi pada sistem keamanan GSM. Algoritma A8 membangkitkan kunci sesi, Kc, dengan melihat random challenge, RAND, yang diterima dari MSC dan kunci rahasia Ki, yang terdapat pada kartu SIM. Algoritma A8 menagmbil 128 bit masukkan dan membangkitkan 64 bit keluaran. Keluaran sejumlah 64 bit ini merupakan kunci sesi Kc.

Nilai Kc ini dapat dibangkitkan oleh MS dan HLR, sehingga BTS dapat menerima nilai Kc yang sama yaitu dari MS dan dari MSC. MSC dapat membangkitkan nilai Kc karena mendapat kiriman dari HLR. Sedangkan HLR dapat membangkitkan nilai Kc karena HLR mengetahui kedua nilai yang dibutuhkan untuk membangkitkan nilai Kc, yaitu RAND (karena yang membangkitkan RAND adalah HLR) dan Ki (karena Ki semua pelanggan pasti diketahui oleh penyedia layanan (operator)). Kunci sesi, Kc, digunakan sampai MSC memutuskan untuk perlu mengautentifikasi MS lagi. Biasanya Kc digunakan sehari penuh setelah proses autentifikasi.



Gambar 3 Perhitungan kunci sesi (Kc)

Baik algoritma A3 maupun A8 disimpan di dalam SIM, yang bertujuan untuk mencegah orang merusak algoritma tesebut. Ini berarti operator dapat memutuskan, algoritma mana yang digunakan secara bebas oleh pembuat perangkat keras dan algoritma mana yang digunakan oleh operator jaringan lain.

3. SERANGAN PADA JARINGAN GSM

Serangan terhadap jaringan GSM sangat berbagai macam, berikut beberapa jenis serangan pada GSM :

3.1. Serangan Brute Force pada A5

Serangan brute force secara *real-time* pada sistem keaman GSM tidak relevan. Hal itu dikarenakan waktu kompleksitas untuk serangan ini sekitar 2^{54} (2^{64} jika semua digit tidak bernilai kosong). Brute force attack membutuhkan waktu yang banyak untuk memungkinkan penyadapan pada panggilan GSM secara *real-time*. Penyadapan mungkin dilakukan dengan melakukan perekaman frame antara MS dan BTS dan melakukan serangan setelah itu.

Jika kita memiliki procesor Pentium III dengan 20 juta transistor dan implementasi untuk satu set LSFRs (A5/1) membutuhkan 2000 transistor, maka kita akan memiliki 10.000 implementasi A/5 secara paralel dalam satu procesor. Jika chip itu memiliki *clocked* 600MHz dan tiap implementasi A5 akan membangkitkan output sebesar satu bit untuk tiap putarannya. Jika kita membutuhkan untuk membangkitkan 100+114+114 bit, kita dapat mencoba 2 Milyar kemungkinan kunci dalam satu detik untuk tiap-tiap implementasi A5/1. Maka untuk jumlah kemungkinan kunci 2^{54} , membutuhkan waktu sekitar 900.000 detik atau setara dengan 250 jam dengan satu procesor. Serangan dapat dioptimalkan dengan melihat pada kunci yang lebih spesifik setelah keystream yang tidak valid pertama. Ini dapat mengurangi kebutuhan waktu sepertiga dari semula. Serangan juga dapat dilakukan dengan multiprocesor, sehingga dapat mengurangi kebutuhan waktu secara drastis sebanding dengan banyaknya penggunaan procesor.

3.2. Serangan Divide and Conquer pada A5

Divide and Conquer yaitu serangan untuk mengurangi

kompleksitas algoritma A5 dari 2^{54} menjadi 2^{45}, sehingga dapat mengurangi sebanyak 29 = 512 kali lebih cepat dari semula. Serangan divide and conquer berdasarkan pada known plainteks attack. Penyerang mencoba untuk mendapatkan inisial state dari LSFRs dari keystrean yang diketahui. Penyerang ingin mengetahui semua nilai keystream bit sebanyak 64 bit. Nilai keystream itu dapat ditemukan jika penyerang mengetahui beberapa cipherteks yang berkorespondensi dengan plainteks. Ini bergantung pada besarnya format frame GSM yang dikirim kembali dan seterusnya. Ftame GSM tediri dari sejumlah informasi yang tetap, contohnya frame header. Kebutuhan untuk menemukan 64 bit tidak dapat selalu dilaksanakan, tetapi 32 sampai 48 bit biasanya ditemukan. Kadang-kadang lebih dari itu. Penyerang hanya membutuhkan 64 bit plainteks.

Pada serangan divide and conquer diimplementasikan dengan menebak isi dari dua LSFRs yang pendek dan menghitung LSFRs yang ketiga dari nilai keystream yang diketahui. Ini dapat dilakukan dengan 2^{40} serangan, jika clock dari dua register pertama tidak bergantung pada register yang ketiga. Karena nilaibit tengah dari register ketiga digunakan dalam clocking, kita harus menebak setengah dari bit pada register ketiga antara clock bit dan LSB. Ini dapat meningkatkan waktu kompleksitas dari 2^{40} menjadi 2^{45}.

J. Golic telah mengajukan divide and conquer yang lain berbasis asumsi yang sama dengan rata-rata kompleksitas dari 2^40.16[2]. Golic menunjukan hanya 2^62.32 inisisal states yang dapat menjangkau dari 2^64 inisial states. Berdasarkan asumsi itu, dia menjelaskan bagaimana mendapatkan persamaan linear dengan menebak n bit pada LSFRs. Dengan menyelesaikan persamaan linerar, satu yang dapat di kembalikan inisial statesnya dari tiga LSFRs. Kompleksitas dari penyelesaian persamaan linear tersebut adalah 2^41.16. Dengan rata-rata, satu dapat menyelesaikan internal state dengan 50 persen kesempatan dalam 2^40.16 operasi. [5]
Golic juga mengajukan serangan Time-Memory Trade-Off berdasarkan Birthday paradox pada paper yang sama[2]. Objektif dari serangan ini untuk mendapatkan internal state dari tiga LSFRs pada waktu yang diketahui dan keystream sequence , kemudian merekonstruksi kunci sesi, Kc.

3.3. Mengakses Sinyal Jaringan

Menurut dua contoh sebelumnya, jelas terlihat bahwa algoritma A5 bukan algoritma yang aman, karena masih memungkinkan serangan dengan *brute-force* dan pada prakteknya, memang algoritma ini tidak aman, karena serangan *brute-force* sebenarnya memang tidak terlalu sulit diimplementasikan pada hardware yang tersedia sekarang yang frekuensinya mencapai sekitar 3000 Mhz. Meskipun algoritma cukup untuk mencegah serangan penyadapan di udara, sehingga gelombang udara antara MS dan BTS menjadi titik persoalan penting pada sistem keamanan GSM.

Sesuai dengan pernyataan sebelumnya , transmisi antara MS dan BTS dienkripsi, tetapi setelah sampai BTS, data tersebut ditransmisikan dalam bentuk plainteks.

Fakta pernyataan di atas membuka kemungkinan baru. Jika penyerang dapat mengakses jaringan sinyal operator, maka penyerang dapat mendengarkan segala sesuatu yang ditransmisikan, termasuk segala sesuatu yang berada dalam panggilan seperti RAN, SRES dan Kc. Jaringan sinyal SS7 yang digunakan oleh jaringan operator GSM benar-benar tidak aman jika penyerang dapat mengakses secara langsung.

Pada skenaraio lain jika penyerang meyerang HLR pada suatu jaringan, maka penyerang dapat mengambil Ki untuk semua pelanggan pada jaringan tersebut.

Mengakses sinyal jaringan memang tidak terlalu sulit. Meskipun BTS biasanya dihubungkan dengan kabel. Tetapi ada beberapa yang dihubungkan melalui gelombang microwave atau satelit. Saluran ini akan mudah untuk diakses dengan peralatan yang baik. Sebagian besar peralatan yang tersedia untuk penyadapan GSM sangat mudah digunakan, dan spesifikasi alat ini tidak melanggar hukum yang berlaku.

Ini menjadi pertanyaan tentang mengapa penyerang ingin memecahkan enkripsi algoritma A5 yang melindungi sesi dari MS tertentu, atau memecahkan enkripsi antara BTS dan BSC (*Basic Station Controller*) dan mencari akses jaringan. Kemungkinan untuk mengakses kabel sangat sulit dilakukan, walaupun hal ini merupakan serangan yang paling nyata dan tidak akan terdeteksi dalam waktu lama, jika dilakukan secara hati-hati. Kemampuan untuk menyadap transmisi data antara BTS dan BSC memungkkinkan penyerang dapat memonitor panggilan telepon dengan menyadap saluran panggilan, atau penyerang dapat mengambil nilai kunci sesi, Kc, dengan memonitor saluran, memotong panggilan di udara dan mendekripsikannya di udara. Sehingga penyerang saat ini mengetahui Kc.

Pendekatan lain yaitu sosial engineering. Pendekatan ini jangan dianggap remeh, meskipun ini kedengaran lucu. Mekanisme penyerangannya yaitu penyerang berpura-pura sebagai tukang service atau sejenisnya, masuk ke dalam gedung dan menginstalasi alat penyadap gelombang. Dia dapat juga menyuap seorang engineer yang bekerja di tempat itu untuk memasang alat penyadap tersebut atau dapat juga meminta engineer tersebut untuk memberinya semua kunci Ki seluruh pelanggan pada operator tersebut.

Kemungkinan menggunakan cara ini sangat kecil, tetapi cara ini merupakan cara yang paling nyata.

3.4 Mengambil Kunci dari SIM

Keamanan dari keseluruhan sistem keamanan GSM terletak pada kunci rahasia, Ki. Jika kunci ini berhasil diperoleh maka seluruh informasi lain mengenai pelanggan yang bersangkutan dapat diperoleh. Sewaktu penyerang mampu untuk mengambil kunci Ki, maka dia tidak hanya mampu mendengarkan panggilan telepon pelanggan, tetapi juga menggunakan panggilan dengan menggunakan nomor pelanggan asli, karena dia dapat menirukan legitimasi pelanggan. Jaringan GSM memiliki gelombang penjegal untuk jenis serangan seperti ini, mekanismenya yaitu jikia dua telepon dengan ID yang sama dijalankan secara bersamaan, dan jaringan GSM mendeteksinya, mencatat lokasi kedua telepon tersebut, mendeteksi ada telepon yang "sama" pada lokasi yang berbeda, maka secara otomatis jaringan GSM akan menutup *account* tersebut, untuk mencegah penyerang melakukan pengkloningan telepon. Tetapi pencegahan seperti ini sangat tidak mangkus jika penyerang hanya ingin mendengarkan panggilan pelanggan.

Grup peneliti dari Pengembang smartcard dan ISAAC(*Internet Security, Applications, Authentication and Cryptography*) melihat adanya cacat pada algoritma COMP128 yaitu dapat secara mangkus untuk mengambil kunci Ki dari SIM [4][5].
Serangan ini berbasis pada *chosen-challenge attack*. Hal ini dikarenakan algoritma COMP128 jika kita mengetahui nilai RAND dan SRES maka kita mengetahui nilai Ki. SIM yang di akses dengan smartcard reader terhubung dengan PC. PC membuat sekitar 150.000 *challenges* ke SIM dan SIM membangkitkan SRES dan kunci sesi, Kc, berdasarkan *challenge* dan kunci Ki. Maka dari itu nilai Ki dapat dideduksi dari SRES response menggunakan diferensial kriptanalisis. Smartcard reader dapat digunakan untuk serangan dengan menghasilkan 6.25 query per detik ke kartu SIM. Sehingga serangan membutuhkan waktu sekitar delapan jam, setelah itu hasilnya dianalsisis. Dengan cara seperti ini penyerang harus dapat mengakses secara fisik SIM yang akan menjadi target selama delapan jam.

Selain itu, kemungkinan ini juga berlaku pada skenario sosial engineering. Kemungkinan itu dapat berupa dealer GSM yang korup akan menggandakan kartu SIM dan menjual kartu tersebut ke pihak ketiga. Kemungkinan lain yaitu mencoba untuk menjual kartu SIM ke seseorang yang bertujuan untuk menguping panggilan telepon. Pihak dealer yang korup tersebut akan memberikan penyerang kartu SIM korban, sehingga penyerang dapat mengkloning kartu SIM tersebut dan digunakan untuk melakukan penyadapan telepon. Ini semua merupakan scenario yang realistis yang memungkinkan untuk memecahkan algoritma COMP128 yang merupakan keamanan terbesar dari seluruh sistem keamanan GSM, sehingga pada akhirnya sistem keamanan GSM tersebut tidak memberikan efek keamanan apapun.

3.5 Mengambil Kunci dari SIM di udara

Serangan udara berdasarkan pada mekanisme antara MS (*mobile station/handphone*) yang membutuhkan respon berupa *challenge* dari jaringan GSM. Jika sinyal dari BTS yang sah di akses oleh penyerang, dan penyerang tersebut mem-bom MS dengan *challenge* dan merekonstruksi kunci rahasia Ki dari respon MS.

Serangan akan dilakukan di tempat dimana sinyal dari BTS yang sah tidak tersedia, tetapi telepon masih hidup. Untuk menghindari pelanggan merasa curiga mengapa baterai teleponnya mudah habis walaupun tidak digunakan telepon, maka penyerang melakukan serangan tidak sekaligus selama delapan jam. Tetapi penyerang melakukan nya selama kurang lebih 20 menit sehari. Setelah SIM dapat dikloning, maka SIM hasil kloning dapat dipakai selama pengguna (korban) masih menggunakan kartu SIM tersebut. Serangan ini dalam prakteknya jarang terjadi.

3.6. Mengambil Kunci dari SIM dari AUC

Penyerangan yang dilakukan guna mengambil kunci Ki dari kartu SIM dapat juga dilakukan untuk mengambil Ki dari AuC. AuC menjawab permintaan dari jaringan GSM dan memberi nilai triplet yang valid yang digunakan untuk proses autentifikasi di MS. Prosedurnya sama dengan prosedur yang digunakan MS untuk mengakses kartu SIM. Perbedaannya adalah AuC lebih cepat dalam memproses pemintaan daripada kartu SIM, hal itu dikarenakan AuC butuh untuk memproses yang lebih banyak permintaan dibanding kartu SIM. Keamanan AuC memegang peranan besar dalam menentukan apakah serangan akan berhasil atau tidak.

3.7. Memecahkan Algoritma A8

Kemungkinan lain untuk memecahkan sistem keamanan pada GSM yaitu dengan memecahkan algoritma A8. Dengan memecah algoritma A8, kita dapat mengambil kunci Ki, berdasarkan pada random challenge, RAND, kunci sesi, Kc, dan SRES response dengan usaha yang minimal. Sebagai contoh, penyerang dapat mencari RAND yang dapat menhasilkan nilai Ki sebagai hasil akhir. Prosesnya yaitu, RAND dan SRES ditransmisikan di udara dalam bentuk plainteks dan kunci sesi Kc dapat diperoleh dengan mudah dari frame terenkripsi dan known plainteks yang cukup. Kemungkinan seperti ini yaitu tentang algoritma pembangkitan kunci harus menjadi bahan pemikiran GSM consortium untuk mendesain algoritma keamanan generasi selanjutnya.

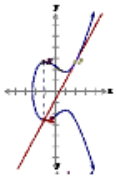
4. *ELLIPTIC CURVE CHRYPTOGRAPHY* (ECC)

ECC merupakan teknik kriptografi asimetri yang menggunakan dua buah kunci berbeda dalam proses enkripsi-dekripsi. Kedua kunci tersebut dikenal dengan *private key*, yang digunakan untuk enkripsi data, dan *public key*, yang digunakan untuk dekripsi data. [2]

Persamaan kurva elips ternomalisasi yang digunakan adalah

$$y^3 \equiv x^3 + -6x + 6 (\mathrm{mod}\, 257) \qquad [2]$$

Pemilihan mod 257 dikarenakan pada sistem ini, metoda pengacakan data dilakukan tiap *byte* dalam suatu koordinat tertentu. Angka maksimal satu *byte* adalah 255, maka bilangan prima terdekat dengan 255 adalah 257.



Gambar 4. Kurva elips untuk persamaan

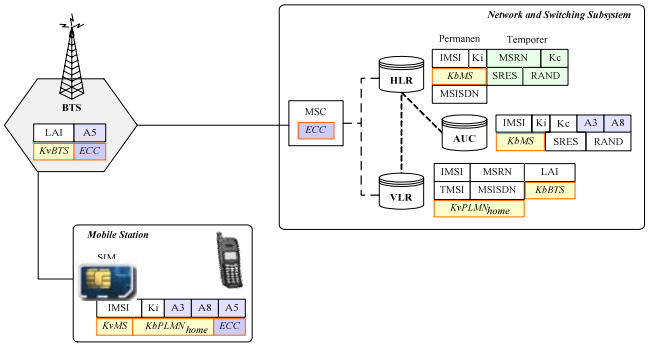
$$y^2 = x^3 - 6x + 6$$

4.1. Keuntungan ECC

Dipilihnya ECC sebagai metoda tambahan untuk mengatasi kelemahan sistem keamanan jaringan GSM berdasarkan pada hal-hal berikut[2]:

1. Besarnya field dimana kurva elips berada dapat dipilih sehingga memudahkan implementasi ECC pada suatu batasan tertentu.
2. Besar kunci yang dihasilkan dengan metoda ECC tidak terlalu besar sehingga tidak membutuhkan banyak memori tambahan.
3. Proses kriptografi ECC tidak membutuhkan prosesor khusus sehingga bisa mengurangi biaya implementasi.

4.2 Pemodelan Sistem Keamanan GSM dengan Metoda ECC



Gambar 5.Distribusi fitur sistem keamanan jaringan GSM dengan metoda ECC

Dengan penambahan metoda ECC pada sistem keamanan jaringan GSM, tentunya diperlukan pula penambahan fitur sistem keamanan pada jaringan GSM. Parameter-parameter ECC yang ditambahkan pada jaringan GSM terlihat seperti pada gambar 5 di atas.

4.3 Analisa *Avalanche Effect*

Salah satu cara untuk menguji ketahanan kriptografi adalah dengan mengukur nilai *avalanche effect* kriptografi tersebut. Nilai *avalanche effect* dirumuskan dengan:

$$Avalanche\_Effect(AE) = \frac{\sum bit\_berubah}{\sum bit\_total} * 100\% \qquad [2]$$

Nilai *avalanche effect* optimal untuk suatu metoda kriptografi adalah 50 %. Pengukuran nilai *avalanche effect* pada tugas akhir ini hanya dilakukan terhadap parameter-parameter yang dikirimkan pada pemodelan prosedur registrasi MS saat berada di PLMN asal yaitu IMSI, RAND, $SRES_{MS}$, Kc, dan TMSI. Pengukuran tidak dilakukan terhadap pemodelan prosedur lainnya sebab hasil telah didapatkan dianggap telah dapat mewakili keseluruhan pemodelan. Pengukuran *avalanche effect* meliputi pengaruh dari perubahan satu bit *plain text*, kunci enkripsi, dan *cipher text*

Dari hasil simulasi yang dilakukan Anastasia Ibrani Sagita, rata-rata nilai *avalanche effect* untuk perubahan satu bit *cipher text* mencapai 50.102 Metoda kriptografi ECC adalah metoda kriptografi asimetris dimana proses enkripsi dan dekripsi menggunakan dua kunci yang berbeda baik ukuran maupun formatnya. Dan begitu pula dengan proses yang terjadi antara enkripsi dan dekripsi, sehingga pola pengacakan yang terjadi akibat adanya perubahan bit input menjadi sangat berbeda. [2]

Dengan nilai rata-rata AE sebesar 50.102 %, metoda kriptografi ECC terbukti memiliki ketahanan yang baik dan bisa diterapkan untuk melindungi parameter-parameter keamanan GSM.

5. KESIMPULAN

Kesimpulan yang dapat diambil dari makalah ini adalah :

1. Enkripsi pada jaringan GSM menggunakan algoritma A3 digunakan untuk melakukan authentifikasi, algoritma A5 digunakan dalam proses penyandian data pengguna dan data sinyaling, dan A8 adalah algoritma untuk menghasilkan kunci yang digunakan dalam proses penyandian.
2. Banyak kemungkinan untuk melakukan serangan pada sistem keamanan GSM, serangan itu dapat dilakukan pada algoritma A3, A5 maupun A8.
3. Dengan nilai rata-rata AE sebesar 50.102 %, metoda kriptografi ECC terbukti memiliki ketahanan yang baik dan bisa diterapkan untuk melindungi parameter-parameter keamanan GSM.

DAFTAR REFERENSI

[1] Golic J. Dr. , Cryptanalysis of Alleged A5 Sream Cipher, *http://jya.com/a5-hack.htm*.

[2] Ibrani Sagita, Anastasia., Uke Kurniawan Usman, Iwan Iwut. 2006 . *Simulasi Penerapan Metode Elliptic Curve Cryptography untuk Mengatasi Kelemahan Sistem Keamanan Jaringan GSM*. Jurusan Teknik Elektro, STT Telkom.

[3] Margrave David, GSM Security and Encryption, *http://www.net-security.sk/telekom/phreak/radiophone/gsm/gsm-secur/gsm-security-and-encryption .html*

[4] Munir, Rinaldi. 2007. Diktat Kuliah IF5054 Kriptografi. Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika , Institut Teknologi Bandung.

[5] Quirke, Jeremy.2004. *Security on GSM System* (e-book). AusMobile, 2004.