STUDI DAN PERBANDINGAN KEAMANAN GSM DAN CDMA

Mohamad Firda Fauzan – NIM : 13504127

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if14127@students.if.itb.ac.id

Abstrak

Perkembangan telepon selular setiap tahun semakin meningkat, baik dari segi kuantitas yaitu pertambahan jumlah pengguna maupun segi kualitas yaitu peningkatan fitur yang disediakan oleh operator. Di lain sisi berdasarkan hasil penelitian pada tahun 2003 menunjukkan 850 juta telepon selular mengalami penyadapan (*eavesdrop*) pada saat terjadi panggilan.

Untuk menjamin aspek keamanan, sistem jaringan GSM (*Global System for Mobile*) menawarkan tiga macam keamanan, yaitu autentifikasi, kerahasiaan data dan sinyal, serta kerahasiaan pengguna. Kebutuhan autentifikasi dilakukan dengan penggunaan *smart card* yang lebih dikenal dengan nama *SIM card*. Kerahasiaan data dan sinyal dilakukan dengan melakukan enkripsi dengan algoritma tertentu, pada 0umumnya pada jaringan GSM digunakan algoritma A3, A5 dan A8. Enkripsi tesebut dilakukan pada data yang ditransfer antara telepon selular dengan BTS (*Base Transceiver Station)*. 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.

Jaringan CDMA (*Code Division Mobile Acces*) menawarkan aspek keamanan yang lebih baik dari jaringan GSM. Sistem CDMA sangat dikenal sebagai sistem telekomunikasi yang mempunyai tingkat keamanan paling tinggi. Terminologi keamanan di sini adalah dari kemungkinan penyadapan (*eavesdrop*) dan penggandaan (*cloning*) oleh orang atau pihak yang tidak mempunyai otorisasi. Hal ini ditunjukkan baik pada sisi lapisan fisik maupun pada lapisan–lapisan di atasnya seperti lapisan data link, lapisan transport maupun lapisan sesi. Di lapisan fisik, sistem CDMA menggunakan metode multiple division dengan code, dimana sinyal data ditumpangkan pada sinyal derau yang tersebar. Di sisi penerima dipasang suatu decoder yang mampu melakukan dekode sinyal transmisi yang diterima sehingga didapat sinyal asli yang dikirimkan. Sedangkan di lapisan yang lebih atas lagi, sistem CDMA memberlakukan otentikasi dengan ketat yang memperkecil kemungkinan untuk ditembus oleh pelanggan yang tidak valid dan perangkat yang tidak mendukung sistem keamanan misalnya terminal yang tidak mendukung *A-key*.

Makalah ini membahas tentang perbandingan antara sistem keamanan pada GSM dengan sistem keamanan pada CDMA, sistem keamanan ini menyangkut teknologi yang digunakan pada GSM dan CDMA, algoritma yang digunakan untuk mengenkripsi data, serta jenis-jenis serangan yang mungkin terjadi pada sistem keamanan itu.

***Kata kunci**: GSM, CDMA, keamanan, SIM card.*

1. Pendahuluan

GSM 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.

Keamanan dan mekanisme autentifikasi yang terdapat pada GSM membuat GSM sebagai jaringan komunikasi yang aman, khususnya jika dibandingkan dengan sistem analog. Bagian yang menjadikan GSM aman yaitu adanya sistem digital yang mengenkripsikan pembicaraan, GMSK (*Gaussian Minimum Shift Keying*) modulasi digital, dan TDMA (*Time Division Multiple Access*). Untuk memotong dan merekonstruksi sinyal GSM diperlukan peralatan yang khusus dan mahal.

Spesifikasi GSM yang di desain oleh konsorsium GSM bersifat rahasia dan hanya didistribusikan hanya untuk perusahaan pembuat telepon selular untuk mengetahui dasar-dasar dari perangkat keras dan perangkat lunak dan hanya untuk operator GSM. Spesifikasi GSM tidak disebarluaskan ke umum untuk mencegah terjadinya pembelajaran tentang proses autentifikasi dan algoritma enkripsi terhadap model keamanan GSM. Konsorsium GSM berdasar atas prinsip keamanan dengan ketidakkenalan, maksudnya adalah algoritma enkripsi akan sulit di pecahkan jika algoritma tersebut tidak dipublikasi.

Menurut suatu komunitas sains, salah satu syarat untuk menjaga keamanan suatu algoritma adalah keamanan pada sistem kriptografinya, ini berarti keamanan hanya terdapat pada kuncinya. Pendapat ini terkenal dengan asumsi Kerckhoffs'. Algoritma seharusnya harus dipublikasi, sehingga algoritma itu dapat diteliti oleh masyarakat umum. Dengan itu dapat diketahui seberapa kuat algoritma tersebut. Kondisi berbeda terjadi jika algoritma tidak dipublikasi, suatu ketika mungkin algoritma tersebut mengalami kesalahan desain sehingga sebenarnya sangat mudah dipecahkan.

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.

CDMA merupakan suatu menggunakan teknologi spread-spectrum untuk mengedarkan sinyal informasi yang melalui bandwith yang lebar (1,25 MHz). Teknologi ini asalnya dibuat untuk kepentingan militer, menggunakan kode digital yang unik, lebih baik daripada channel atau frekuensi RF.

CDMA memiliki tingkat keamanan lebih baik dari jaringan GSM, hal ini disebabkan karena sistem CDMA menggunakan metode multiple division dengan code, dimana sinyal data ditumpangkan pada sinyal derau yang tersebar. Di sisi penerima dipasang suatu decoder yang mampu melakukan dekode sinyal transmisi yang diterima sehingga didapat sinyal asli yang dikirimkan. Sedangkan di lapisan yang lebih atas lagi, sistem CDMA memberlakukan otentikasi dengan ketat yang memperkecil kemungkinan untuk ditembus oleh pelanggan yang tidak valid dan perangkat yang tidak mendukung sistem keamanan misalnya terminal yang tidak mendukung *A-key*

Sistem CDMA yang diaplikasikan saat ini di Indonesia adalah CDMA2000-1X yang merupakan perkembangan dari teknologi selular CDMA2000 sebelumnya. Pada sistem CDMA, keamanan informasi merupakan hal yang sangat *concern* untuk diperhatikan. Masalah seperti penyadapan dan penggunaan akses secara tidak sah sangat diperhatikan.

CDMA2000-1X menggunakan teknik enkripsi dengan algoritma Rijndael yang aman dan sangat cepat dan hanya memungkinkan penggunaan ukuran kunci 128, 192 and 256 bit. Sedangkan pada autentifikasi menggunakan prosedur

Unique Challenge Procedure dimana *base station* membangkitkan nilai 24 bit *value* dan mentransmisikannya ke *mobile station* di *Authentication Challenge Message.* Teknologi CDMA membuat kesulitan terhadap kegiatan penyadapan, baik yang bersifat terus menerus maupun sesaat karena mengimplementasikan 42 bit PN (*Pseudo-Random Noise*) sekuens yang disebut dengan "*Long Code"*

Selain itu, untuk memberikan jaminan keamanan informasi dan fleksibilitas pada pelanggan, pihak operator memanfaatkan teknologi smart card yaitu berupa kartu RUIM (*Removable User Identity Module*) yang merupakan pengembangan dari teknologi kartu SIM (*Subcribers Identity Module*) pada sistem GSM. RUIM digunakan sebagai identitas bagi user untuk melakukan fungsi autentikasi, otorisasi dan pelaporan, serta memberikan fleksibilitas bagi pelanggan. RUIM memiliki spesifikasi khusus yang terdiri dari struktur fisik, sistem elektrik dan pensinyalan dan struktur logika. RUIM merupakan mikrokomputer yang dapat mengolah informasi data dalam format biner. Didalamnya terdapat mikroprosesor, sistem memori dan sistem operasi dengan fungsi utamanya sebagai jalur untuk mengakses jaringan.

Pada makalah ini, saya akan memaparkan tentang sistem keamanan pada GSM, sistem keamanan pada CDMA, serta perbandingan keamanan antara GSM dengan CDMA.

2. Jaringan GSM

GSM (Global System for Mobile) 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.

2.1 Aspek Keamanan yang disediakan GSM

GSM menawarkan 3 aspek keamanan yaitu :

1. Autentifikasi pengguna.
   Yaitu kemampuan telepon selular untuk membuktikan apakah yang melakukan akses adalah pengguna yang sah.
2. Kerahasiaan data dan sinyal.
   Yaitu proses mengenkripsi pesan dan data yang di transmisikan.
3. Kerahasiaan pengguna.
   Yaitu sewaktu jaringan butuh identitas pelanggan atau selama proses autentifikasi IMSI (International Mobile Subscribe Identity) yang unik tidak dalam bentuk plainteks (sudah terenkripsi).

2.2. Arsitektur jaringan GSM

Bagian arsitektur jaringan GSM yang terkait dengan sistem keamanan adalah m*obile station* (MS), *Base Station Subsistem* (BSS), dan *Network and Switching Subsistem* (NSS)

- ***Mobile Station* (MS)**
- ***Mobile Equipment* (ME)**

ME adalah perangkat fisik yang digunakan untuk berkomunikasi. Fitur keamanan yang terdapat di dalam ME adalah *International Mobile Equipment Identity* (IMEI) yang berfungsi sebagai identitas ME. Adanya IMEI memungkinkan operator memastikan bahwa bukan ME curian atau ME yang tidak terdaftar yang digunakan.

- ***Subscriber Identity Module* (SIM)**

SIM adalah sebuah *smart card* yang mengidentifikasikan MS didalam jaringan. Data-data yang berkaitan dengan sistem keamanan GSM didalam SIM adalah:

- Identitas pelanggan berupa IMSI yang merupakan identitas utama dari sebuah MS dan MSISDN (*Mobile Station* ISDN)
- PIN (*Personal Identification Number*)
- Kunci autentikasi Ki, dan algoritma A3,A5, dan A8
- Ki adalah kunci autentifikasi dengan panjang 128 bit yang berfungsi untuk membangkitkan 32 bit response pada proses autentifikasi yang disebut SRES.

- ***Base Station Subsistem* (BSS)**

BSS terdiri dari *Base Station Controller* (BSC) dan *Base Transceiver Station* (BTS). Proses enkripsi – dekripsi data dengan menggunakan algoritma A5 terletak di BTS.

- ***Home Location Register* (HLR)**

HLR adalah *database* utama yang digunakan untuk menyimpan semua data yang berhubungan dengan pelanggan. Ada dua jenis parameter keamanan yang disimpan di HLR yaitu data permanen yang terdiri dari IMSI dan kunci

autentikasi Ki, serta data temporer yang terdiri dari RAND, SRES, dan kunci penyandian Kc.

- ***Authentication Centre*** **(AUC)**

AUC menyimpan data-data yang diperlukan untuk mengamankan komunikasi pada jalur radio terhadap berbagai gangguan. Data-data tersebut adalah data autentikasi yang berupa IMSI dan Ki, RAND, SRES, Kc, serta algoritma A3 dan A8.

- ***Visitor Location Register*** **(VLR)**

VLR adalah suatu *database* yang memuat informasi dinamis tentang seluruh MS yang sedang berada dalam area pelayanan MSC. Fungsi VLR yang berkaitan dengan sistem keamanan GSM adalah:

- Bekerja sama dengan HLR dan AUC untuk proses autentikasi.
- Meneruskan pengiriman kunci penyandian Kc dari HLR ke BSS untuk proses enkripsi/dekripsi.
- Mengontrol alokasi pemberian nomor TMSI baru. Nomor TMSI berubah-ubah secara periodik untuk melindungi identitas pelanggan.

2.3. Layanan sistem keamanan GSM

Berdasarkan ETSI 02.09, terdapat empat layanan dasar sistem keamanan GSM, yaitu alokasi TMSI, autentikasi, penyandian (enkripsi/dekripsi data), serta identifikasi ME dan modul SIM.

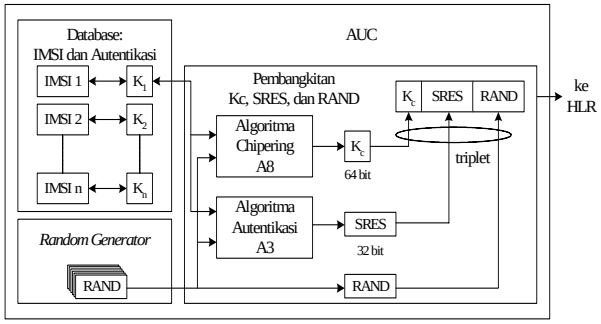
2.3.1. Alokasi TMSI

Identitas pelanggan dirahasiakan dengan tidak mengirimkan IMSI melalui *interface* radio jika dalam keadaan normal. IMSI dikirimkan hanya pada saat pertama kali pelanggan mengakses jaringan dan apabila jaringan kehilangan korelasi antara IMSI dengan TMSI (*Temporary Mobile Subscriber Identity*). TMSI adalah pengganti IMSI yang diberikan oleh VLR. TMSI bersifat sementara, berubah-ubah secara acak pada setiap *location update*, dan dikirimkan dalam keadaan terenkripsi oleh algoritma A5.

2.3.2. Autentikasi

Autentikasi identitas pelanggan bertujuan untuk mengetahui apakah pelanggan tersebut terdaftar dalam *database* jaringan atau tidak. Proses autentikasi ini diperlukan selama registrasi lokasi MS, l*ocation update* dengan perubahan VLR, dan c*all setup*

Mekanisme autentikasi dalam GSM dikenal dengan nama metoda *Challenge– Response*, yaitu teknik autentifikasi dengan cara memberikan *challenge* (RAND) kepada pelanggan untuk menghasilkan suatu informasi tertentu (*response*-SRES). Autentikasi tersebut melibatkan serangkaian parameter RAND, SRES, dan Kc yang disebut *triplet*. Di sisi jaringan, triplet dihasilkan secara simultan di AUC.

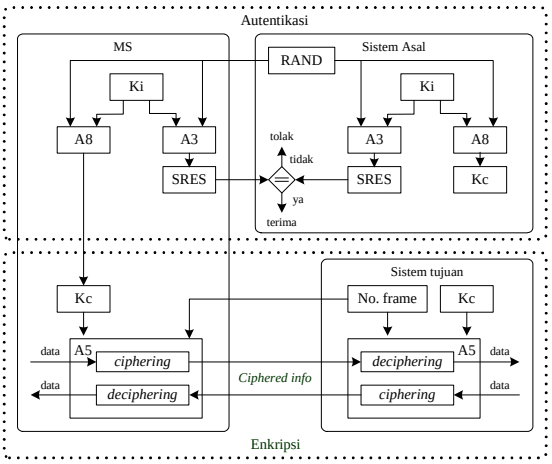


Gambar 1 Proses pembangkitan Triplet

2.3.4. Penyandian data

Enkripsi data dengan algoritma A5 bisa dilakukan setelah proses autentikasi pelanggan, yakni setelah MS yang mengakses jaringan terbukti legal sebagai pelanggan GSM.

Proses penyandian data yang terjadi di MS sama persis dengan yang terjadi di BTS. Karena menggunakan kunci yang sama maka sepasang *codeword* yang dihasilkan dari algoritma inipun juga sama. Proses enkripsi menggunakan *codeword* untuk membentuk *cipher text* yang akan dikirimkan, sedangkan proses dekripsi menggunakan *codeword* untuk mendapatkan *plain text* kembali.

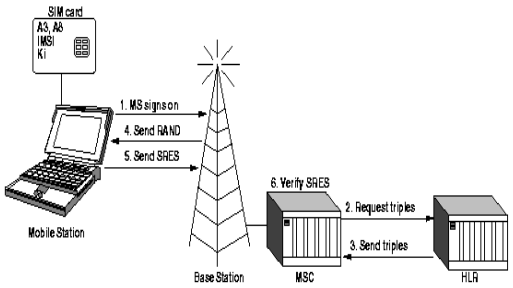


Gambar 2 Proses autentifikasi dan enkripsi

2.4. Mekanisme sistem keamanan GSM

Sistem keamanan GSM berdasar pada pertukaran data antara HLR (Home Location Register) dengan kartu SIM pada MS (Mobile Station atau telepon selular). Data yang ditukarkan diatas yaitu Ki, yaitu kunci sepanjang 128 bit yang digunakan untuk membuat 32 bit response yang disebut SRES, sebagai jawaban dari adanya random challenge yang disebut RAND, yang dikirim MSC melalui BTS kepada MS. Selain Ki data yang ditukarkan yaitu Kc, yaitu kunci sepanjang 64 bit yang digunakan untuk mengenkripsi pesan selama di udara antara BTS dengan MS. RAND, SRES yang dibangkitkan berdasarkan adanya RAND dan Ki, serta Kc yang juga dibangkitkan berdasarkan Ki disebut triplet, yang triplet tersebut telah dijelaskan di bagian makalah sebelumnya dalam proses autentifikasi.

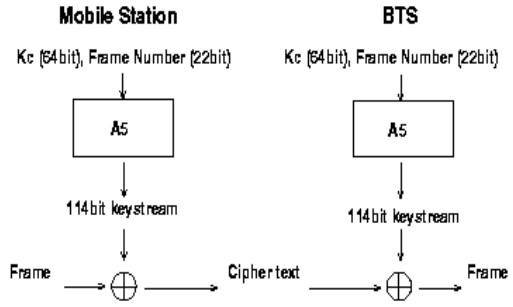
Proses autentifikasi dimulai dengan adanya MS *sign on* MSC (Mobile Service Switching Center) melalui BTS dengan mengirim identitas, kemudian MSC meminta triplet kepada HLR, lalu HLR memberi HLR kepada MSC. MSC mengirim RAND kepada MS, kemudian MS menghitung SRES dengan algoritma A3 menggunakan RAND yang diterima dan Ki yang terdapat pada SIM. Setelah itu MS mengirim SRES kepada MSC. MSC menerima SRES, lalu mencocokkan SRES dengan SRES dari triplet dari HLR (HLR dapat menghitung SRES dari RAND yang HLR buat, karena HLR mengetahui semua Ki pada SIM).



Gambar 3 Mekanisme autentifikasi

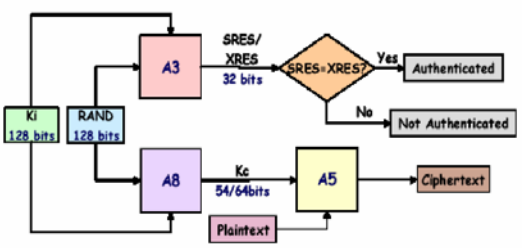
Setelah proses autentifikasi selesai, MS membangkitkan kunci sesi, Kc, dengan algoritma A8 berdasarkan pada *challenge* dari MSC dan Ki. Begitu juga pada BTS yang berfungsi sebagai sarana komunikasi dengan BTS, menerima Kc dari MSC, sehingga proses komunikasi udara antara BTS dengan MS terenkripsi.

Setiap frame dienkripsi dengan *keystream* yang berbeda. Keystream ini di bangkitkan dengan algoritma A5. Algoritma A5 diinisialisasi dengan Kc dan jumlah frame yang akan dienkripsi., kemudian membangkitkan keystream yang berbeda untuk setiap frame. Ini berarti suatu panggilan dapat didekripsi jika penyerang mengetahui Kc dan jumlah dari frame. Kc yang sama digunakan selama MSC belum mengautentifikasi MS lagi.



Gambar 4 Enkripsi dan dekripsi frame

Berikut ringkasan dari algoritma yang digunakan dalam GSM



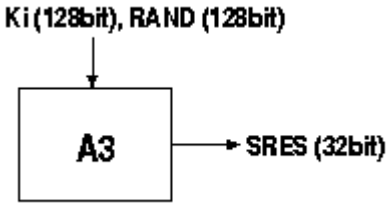
Gambar 5 Skema algoritma yang digunakan oleh sistem GSM

2.5 Algoritma Kriptografi GSM

2.5.1 Algoritma A3, Algoritma autentifikasi.

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

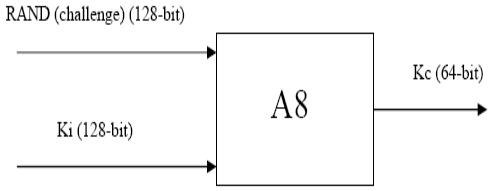
Dalam waktu dekat setiap operator GSM di seluruh dunia akan menggunakan algoritma yang disebut COMP128 sebagai penggabungan algoritma A3 dan A8. COMP128 adalah algoritma yang sudah disepakati dalam konsorsium GSM. Algoritma lain pun sudah bermunculan, tetapi semua operator akan menggunakan COMP128.

COMP128 memiliki mekanisme seperti algoritma A3 pada gambar 6, tetapi COMP128 membangkitkan nilai 128 bit, dimana 32 bit awalnya merupakan SRES seperti pada algoritma A3.

2.5.2 A8, Algoritma untuk membangkitkan nilai kunci sesi (Kc)

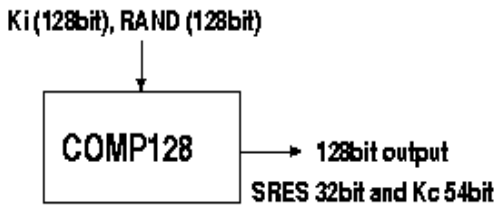
Algoritma A8 adalah algoritma yang berfungsi untuk membangkitkan kunci sesi pada sistem keamanan GSM. Algoritma A8 membangkitkan kunci sesi, Kc, dengan melihat random challenge, RAND, yang diterima dari MSC dan kunci rahasia Ki, yang terdapat pada kartu SIM. Algoritma A8 menagmbil 128 bit masukkan dan 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 7 Perhitungan kunci sesi (Kc)

Seperti yang sudah dijelaskan di subbab sebelumnya, 2.5.1, COMP128 menggunakan kedua algoritma yaitu algoritma A3 dan A8. Algoritma COMP128 membangkitkan SRES dan kunci sesi, Kc, dalam satu waktu. Hasil dari COMP128 adalah 32 bit awal merupakan SRES dan 54 bit akhir merupakan kunci sesi, Kc, sampai MS kembali diautentifikasi.



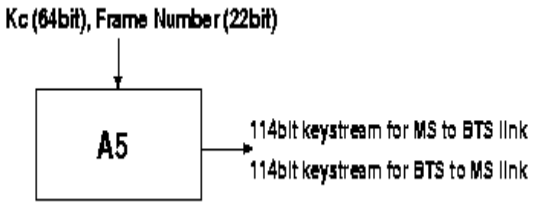
Gambar 8 Perhitungan algoritma COMP128

COMP128 menghasilkan kunci sesi, Kc, sepanjang 54 bit yang seharusnya 64 bit jika dibangkitkan dengan algoritma A5. Sepuluh bit nol ditambahkan ke kunci sesi. Kc, yang dibangkitkan COMP128, sehingga diperoleh kunci sepanjang 64 bit yang mana 10 bit terakhirnya merupakan bit-bit nol. Hal ini efektif untuk mengurangi perbedaan kunci dari 64 bit ke 54 bit. Hal ini adalah prinsip yang digunakan di semua implementasi algoritma A8.

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.

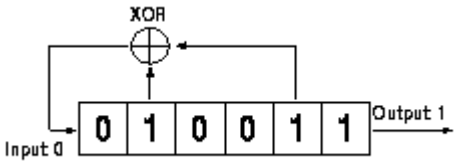
2.5.3 A5/1, Algoritma untuk mengenkripsi pesan selama di udara

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*.

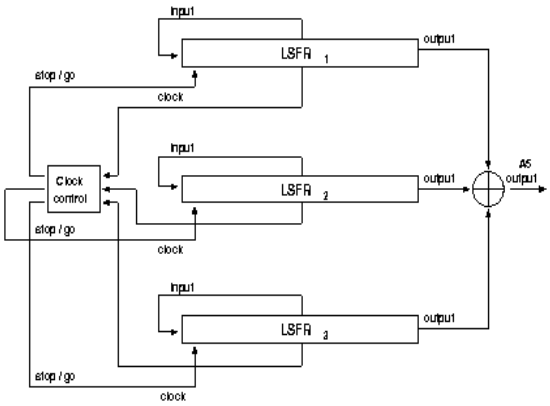


Gambar 9, Pembakitan Keystream

Algoritma A5 yang digunakan di negara-negara Eropa terdiri dari tiga LSFRs dari tiga panjang yang berbeda. Pada gambar 10, kombinasi tiga panjang LSFRs adalah 64 bits. Output dari tiga register yang di LSFRs tersebut di XOR kan secara bersamaan dan hasil XOR menggambarkan satu keystream bit.LSFR tersebut memiliki panjang 19, 23, dan 23 bit dengan beberapa *feedback* yang polinomial. Ketiga register tersebut dijadwalkan berdasarkan pada bit tengah pada register. Register dijadwalkan jika bit tengahnya sesuai dengan nilai mayoritas dari tiga bit tengah register lainnya.. Contoh, jika bit tengah dari tiga register tersebut masing-masing 1,1 dan 0, maka dua register pertama dijadwalkan, atau contoh lain bit tengah masing-masing register adalah 0, 1 dan 0 maka register pertama dan ketiga dijadwalkan. Karena itu, maka minimal dua register dijadwalkan bersamaan dalam setiap putaran. Untuk lebih jelasnya lihat gambar 11.



Gambar 10 Contoh LSFR dengan feedback polynomial.



Gambar 11 Konstruksi LSFR pada A5

Tiga LSFRs pada gambar diatas diinisialisasi dengan kunci sesi dan jumlah frame. Mekanisme kerjanya yaitu, pertama 64 bit Kc di load ke

dalam register bit demi bit, LSB (Left Significant Bit/ bit paling kiri) dari kunci di XORkan dengan masing-masing LSFRs. Semua register dijadwalkan secara bersamaan (aturan mayoritas penjadwalan seperti dijelaskan di atas dinonaktifkan). Semua bit dalam Kc yaitu sejumlah 64 bit di load ke dalam register secara bersamaan. Bit-bit yang menyatakan jumlah frame sebanyak 22 bit juga diload ke dalam register secara bersamaan, kecuali jika aturan penjadwalan iaktifkan dari sekarang. Setelah semua register telah diinisialisasi dengan Kc dan jumlah frame, register tersebut dijadwalkan seratus kali dan pembangkitan keystream bit dihentikan. Hal ini dilakuka sewaktu mencampur frame number dan mengunci material bersamaan. Sekarang 228 bit dari keluaran keystream dibangkitkan. Keystream sejumlah 228 bit tersebut dapat dikategorikan denga 114bit digunakan untuk mengenkripsi frame dari MS ke BTS dan 114 bit sisanya digunakan untuk mengenkripsi frame dari BTS ke MS. Setelah itu algoritma A5 diinisialisasi kembali dengan kunci sesi, Kc, yang sama dan jumlah frame berikutnya.

Sejak pertama kali jaringan GSM ada, algoritma selain A5 telah didesain dan diimplementasikan. Motivasi utamanya karena algoritma enkripsi A5 yang orisinil sangat sulit untuk diterapkan di timur tengah. Sehingga algoritma A5 yang orisinil diganti namanya dengan A5/1. Algoritma lain yang termasuk di dalamnya yaitu A5/0, yang berarti tidak ada enkripsi sama sekali, dan A5/2, algoritma udara lemah. Secara umum, algoritma A5 setelah A5/1 memiliki nama A5/x. Sebagian besar algoritma A5/x lebih lemah dibandingkan dengan algoritma A5/1, yang mana waktu kompleksitasnya 2^{54} seperti yang telah diperlihatkan di atas. Perkiraan waktu kompleksitas A5/2 lebih rendah yaitu 2^{16}. Enkripsi ini digunakan di USA. Sedangkan untuk algoritma A5 yang lain tidak terapat fakta tentang mereka, sehingga yang diketahui hanya perkiraan dan asumsi.

Dari uraian di atas dapat disimpulkan karakteristik A5 yaitu :

- A5 adalah stream cipher yang terdiri dari tiga clock yang dikontrol oleh LSFRs dengan derajat 19, 22, dan 23
- Kontrol clock difungsikan dengan melihat bit-bit tengah dari ketiga register.
- Jumlah dari masing-masing derajat register tersebut adalah 64 bit. Kunci sesi sejumlah 64 bit digunakan untuk menginisialisasi register.
- Jumlah frame sebanyak 22 bit dimasukkan ke dalam register.
- Dua keystream dengan panjang 114 bit dibuat untuk tiap frame, yang mana di XORkan dengan saluran atas dan bawah

2.6 Jenis-jenis Serangan pada Jaringan GSM

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

2.6.1 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.

2.6.2 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.

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.

2.6.3 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 mmbuka 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.

2.6.4 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.

2.6.5 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.

2.6.6 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.

2.6.7 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.

3. Jaringan CDMA

CDMA (Code Division Multiple Acces) merupakan suatu menggunakan teknologi spread-spectrum untuk mengedarkan sinyal informasi yang melalui bandwith yang lebar (1,25 MHz). Teknologi ini asalnya dibuat untuk kepentingan militer, menggunakan kode digital yang unik, lebih baik daripada channel atau frekuensi RF.

Jaringan CDMA menawarkan aspek keamanan jaringan dengan mengembangkan algoritma enkripsi. Untuk teknik enkripsi digunakan algoritma Rijndael yang aman dan sangat cepat, pada autentifikasi menggunakan prosedur *Unique Challenge Procedure* dimana *base station* membangkitkan nilai 24-bit *value* dan mentransmisikannya ke *mobile station* di *Authentication Challenge Message*. Teknologi CDMA membuat kesulitan terhadap kegiatan penyadapan, baik yang bersifat terus menerus maupun sesaat karena mengimplementasikan 42-bit PN (*Pseudo-Random Noise*) sekuens yang disebut dengan "*Long Code"*

3.1 Aspek Keamanan yang disediakan CDMA

CDMA menawarkan 3 aspek keamanan yaitu :

1. Autentifikasi
2. Proteksi
3. Anonimity

Autentifikasi

Autentifikasi merupakan proses dimana informasi dipertukarkan antara *mobile station* dan *base station* untuk mengkonfirmasikan identitas mobile station. Prosedur autentifikasi dibawa dari CDMA 2000. *Base station* memiliki *Secret Shared Data* (SSD) yang mana unik untuk setiap *mobile station*. Jika kedua-duanya yakni *base station* dan *mobile station* memiliki set SSD yang identik, prosedur autentifikasi diperkirakan dapat sukses. Prosedur autentifikasi signature (*Auth_Signature*) digunakan untuk menampilkan autentifikasi untuk *mobile station* tertentu. Parameter input berikut ini merupakan syarat dalam prosedur ini yakni:

- RAND_CHALLENGE
- ESN
- AUTH_DATA
- SSD_AUTH
- SAVE_REGISTERS

Autentifikasi ditampilkan menggunakan prosedur *Unique Challenge Procedure*. Dalam prosedur ini, base station membangkitkan nilai 24-bit value dan mentransmisikannya ke *mobile station* di *Authentication Challenge Message*. Tergantung pada catatan pesan, *mobile station* melaksanakan prosedur *Auth_Signature* dan field AUTHU dibangkitkan, yang mana telah dikirim ke *base station* melalui *Authentication Challenge Response Message*. *Base station* juga melaksanakan prosedur *Auth_Signature* menggunakan nilai yang disimpan secara internal,

dan *output* dibandingkan dengan nilai AUTHU pada PDU yang diterima. Jika autentifikasi gagal, maka akses selanjutnya melalui *mobile station* ditolak dan prosedur *updating* SSD dapat dilakukan.

Desain teknologi CDMA membuat kesulitan terhadap kegiatan penyadapan, baik yang bersifat terus menerus maupun sesaat. Hal yang unik dari sistim CDMA adalah 42-bit PN (*Pseudo-Random Noise*) sekuens yang disebut dengan "*Long Code*" ke perebutan suara dan data. Pada *forward* link (jaringan ke *mobile*), data diperebutkan pada *rate* 19.2 Kilo simbol per detik (Ksps) dan pada *reverse link* , data diperebutkan pada *rate* 1.2288 Mega chips per detik (Mcps).

Protokol jaringan keamanan CDMA berada pada 64-bit *authentication key* (A-Key) dan *Electronic Serial Number* (ESN) dari *mobile*. Angka acak yang disebut *RANDSSD* yang dibangkitkan pada HLR/AC, juga menjalankan peran dalam prosedur *authentication*. *A-Key* diprogram dalam mobile dan disimpan dalam *Authentication Center (AC*) jaringan. Sebagai tambahan pada *authentication*, yakni bahwa *A-Key* digunakan untuk membangkitkan sub-key untuk *privacy* suara dan *message encryption.*

CDMA menggunakan standarisasi algoritma CAVE (*Cellular Authentication dan Voice Encryption*) untuk membangkitkan 128-bit *sub-key* yang disebut "*Shared Secret Data*" (SSD). A*Key*, *ESN* dan jaringan-supplied *RANDSSD* merupakan input ke CAVE yang membangkitkan SSD. SSD memiliki dua bagian: SSD_A (64 bit), untuk membuat *authentication signatures* dan SSD_B (64 bit), untuk membangkitkan kunci untuk *encrypt* pesan suara dan signal. SSD dapat di *share* dengan memberikan layanan untuk memungkinkan *local authentication*. SSD yang baru dapat digenerate ketika *mobile* kembali ke jaringan *home* atau *roam* ke sistem yang berbeda.

Jaringan CDMA, *mobile* menggunakan SSD_A dan broadcast RAND* sebagai input terhadap algoritma CAVE untuk membangkitkan 18-bit *authentication signature* (*AUTH_SIGNATURE),* dan mengirimkan ke *base station*. *Signature* ini juga kemudian digunakan oleh *base station* untuk memverifikasi legitimasi *subscriber*. Baik prosedur *Global Challenge* (dimana semua *mobile* merupakan *challenged* dengan jumlah *random* yang sama) dan *Unique Challenge* (dimana spesifik RAND digunakan untuk setiap permintaan *mobile*) dapat diperoleh operator untuk *autentifikasi*. Metode *Global Challenge* memungkinkan terjadi *autentication* dengan sangat cepat. Juga, baik *mobile* dan *track* jaringan *Call History Count* (6-bit counter). Hal ini memberikan jalan untuk mendeteksi terjadinya pengkloningan, sebagaimana operator mendapat sinyal jika ada gangguan.

A-Key dapat diprogram ulang, tapi *mobile* dan jaringan *Authentication Center*harus diupdate. A-Key kemungkinan dapat diprogram oleh salah satu dari vendor berikut:

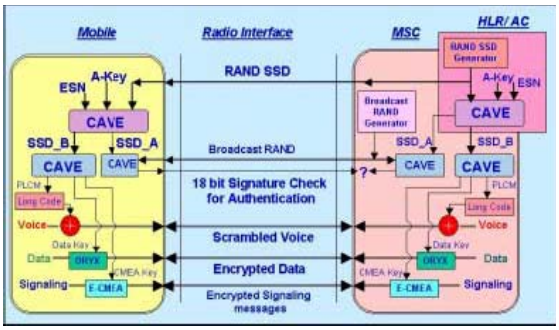
a) Pabrik
b) Dealer pada point penjualan
c) Subscriber via telepon
d)OTASP (over the air service provisioning).

Transaksi OTASP memanfaatkan 512-bit perjanjian algirtma Diffie -Hellman key, membuat aman secara fungsi. A-Key pada mobile dapat diubah melalui OTASP, memberikan cara yang mudah agar cepat memotong layanan (*cut off service*) untuk di kloning secara *mobile* atau membuat layanan baru untuk melegitimasi subscriber. Keamanan A-Key merupakan komponen terpenting dalam sistim CDMA.

3.1.2 Proteksi (Voice, Signal, Data Privacy)

Mobile menggunakan SSD_B dan algoritma CAVE untuk membangkitkan *Private Long Code Mask* (diturunkan dari nilai intermediate yang disebut *Voice Privacy Mask* , yang mana menggunakan sistim legacy TDMA), *Cellular Message Encryption Algorithm* (CMEA) key (64 bits), dan Data Key (32 bits). *Private Long Code Mask* memanfaatkan *mobile* dan jaringan untuk mengubah karakteristik *Long code*. Modifikasi *Long code* ini digunakan untuk penyadapan, yang mana menambahkan extra level privacy melalui CDMA interface udara. *Private Long Code Mask* tidak mengenkripsi informasi, hal ini mudah memindahkan nilai yang telah dikenal dengan baik dalam mengencode sinyal CDMA dengan nilai private yang telah dikenal baik untuk mobile maupun jaringan. Hal ini sangat ekstrim sulit untuk menyadap percakapan tanpa tahu *Private Long Code Mask*. Sebagai tambahan, *mobile* dan jaringan menggunakan key CMEA dengan algoritma Enhanced CMEA (ECMEA) untuk mengenkripsi pesan sinyal dikirim melalui udara dan di dekripsi informasi yang diterima. Kunci data terpisah, dan algoritma enkripsi disebut ORYX, digunakan oleh mobile dan

jaringan untuk mengenkripsi dan mendekripsi lalu lintas data pada saluran CDMA.



Gambar 12 Ilustrasi Autentifikasi dam mekanisme enksripsi pada CDMA

Desain semua telepon CDMA menggunakan kode PN (Pseudo-random Noise) yang unik untuk memperluas sinyal, yang mana hal ini membuat sinyal menjadi sulit untuk disadap.

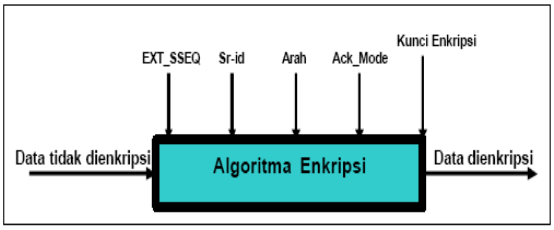
3.1.3 Anonimity

Sistem CDMA mendukung penempatan Temporary Mobile Station Identifier (TMSI) ke dalam telepon, yang berguna untuk mewakili komunikasi ke dan dari suatu telepon selama transmisi udara. Fitur ini membuat kesulitan tambahan untuk menghubungkan antara transmisi telepon pengguna dengan telepon pengguna.

Enkripsi pada CDMA

Teknik enkripsi yang digunakan dalam sistem 1xEV-DV sama dengan yang digunakan pada CDMA2000. *Mobile station* mengindikasikan ke *base station*, beberapa variasi algoritma enkripsi yang mendukungnya. *Base station* mempunyai keleluasaan untuk memutar *on/off* enkripsi sinyal data atau informasi data pengguna. *Mobile station* juga dapat mengusulkan untuk memutar enkripsi menjadi *on/off*. Pesan-pesan tidak dienkripsi jika autentifikasi tidak ditampilkan untuk pesan khusus. Selain itu juga, pesan-pesan yang pendek dikirimkan tanpa dienkripsi. Pesan-pesan yang membawa kapasitas *field* enkripsi cukup bervariasi berdasarkan nilai P_REV dari *mobile station*. Algoritma enkripsi yang digunakan 1xEV-DV adalah *Rijndael Encryption Algorithm*.

Algoritma enkripsi Rijndael merupakan algoritma yang aman dan sangat cepat. Algoritma enkripsi Rijndael memungkinkan hanya ukuran kunci 128, 192 dan 256-bit. Kunci yang digunakan sudah dikembangkan untuk pengaturan *n* round keys. Oleh sebab itu, input data berjalan dengan operasi *rounds*. Algorithm yang digunakan untuk enkripsi dispesifikasikan melalui field SDU_ENCRYPT_MODE variasi pesan layer 3. Jika enkripsi ditampilkan dalam yang ditransmisikan pada layer 3, maka menggunakan SDU, sebagaimana panjangnya menjadi terintegral multiple 8. 8-bit CRC dihitung pada data dan bit-bit CRC dilampirkan pada data. Kombinasi data ini kemudian dienkripsi menggunakan algoritma yang dijelaskan diatas.



Gambar 13 Enkripsi dalam CDMA 1xEV-DV

Tabel 1 Field Enkripsi

Field	Penjelasan
EXT_SSEQ	32 bit urutan jumlah enkripsi keamanan untuk enkripsi/dekripsi
Sr_id	*Identifier* Layanan Referensi untuk pilihan layanan cepat yang terkait
Arah	Arah data yang dienkripsi/dekripsi. Hal itu di set dengan “0” jika data diterima/dikirim pada kanal pengiriman, selain itu di set “1”
Kunci Enkripsi	Kunci sesion untuk enkripsi. Hal ini merupakan hasil sukse perjanjian kunci Sesion antara mobile station dan base station
Ack_mode	Mode pengiriman pesan. Hal ini diatur dengan set “0” jika pesan terkirim menggunakan mo de un-assured, dan yang lainnya di set “1”

4. Keunggulan Teknologi CDMA

Teknologi CDMA memiliki keunggulan dalam beberapa hal, yaitu :

1. Teknologi CDMA didesain tidak peka terhadap interferensi. Di samping itu, sejumlah pelanggan dalam satu sel dapat mengakses pita spektrum frekuensi secara bersamaan karena mempergunakan teknik pengkodean yang tidak bisa dilakukan pada teknologi GSM. Kapasitas yang lebih tinggi untuk mengatasi lebih banyak panggilan yang simultan per channel dibanding sistem yang ada. Sistem CDMA menawarkan peningkatan kapasitas melebihi sistem AMPS analog sebaik teknologi selular digital lainnya. CDMA menghasilkan sebuah skema spreadspectrum yang secara acak menyediakan bandwith 1.250 KHz yang tersedia untuk masingmasing pemanggil 9600 bps bit rate.
2. Dari segi keamanan panggilan, keamanan menjadi sifat dari pendekatan spread spectrum CDMA, dan kenyataannya teknologi ini pertama dibangun untuk menyediakan komunikasi yang aman bagi militer.
3. Mereduksi derau dan interferensi lainnya.
4. CDMA menaikkan rasio signal-to-noise, karena lebarnya bandwith yang tersedia untuk pesan. Efisinsi daya dengan cara memperpanjang daya hidup baterai telepon
5. Salah satu karakteristik CDMA adalah kontrol power sebuah usaha untuk memperbesar kapasitas panggilan dengan mempertahankan kekonstanan level daya yang diterima dari pemanggil bergerak pada base station. Fasilitas kordinasi seluruh frekuensi melalui base-station base station.
6. Sistem CDMA menyediakan soft hand-off dari satu base-station ke lainnya sebagai sebuah roaming telepon bergerak dari sel ke sel,melakukan soft handoff mengingat semua sistem menggunakan frekuensi yang sama.
7. Fungsi spread-spectrum dan power-control yang memperbesar kapasitas panggil CDMA mengakibatkan bandwith yang cukup untuk bermacam-macam layanan data multimedia, dan skema soft hand-off menjamin :
    - ✓ Tidak hilangnya data.
    - ✓ Meningkatkan kualitas suara
    - ✓ Memperbaiki karakteristik cakupan yang dapat menurunkan jumlah sel.
    - ✓ Meningkatkan privacy dan security.
    - ✓ Menyederhanakan perencanaan sistim
    - ✓ Memerlukan daya pancar yang lebih rendah, sehingga waktu bicara ponsel dapat lebih lama.
    - ✓ Mengurangi interferensi pada sistim lain
    - ✓ Lebih tahan terhadap multipath.
    - ✓ Dapat dioperasikan bersamaan dengan teknologi lain (misal AMPS).

5. Kesimpulan

Berikut kesimpulan dari perbandingan jaringan GSM dan CDMA:

1. Baik Jaringan GSM maupun CDMA sama-sama melakukan autentifikasi pada saat awal melakukan panggilan. Autentifikasi pada GSM yaitu menggunakan algoritma A3 dengan kunci Ki dengan metode *Challenge* and *Response*. Sedangkan pada CDMA menggunakan SSD yang unik untuk setiap *mobile station*, autentifikasi menggunakan prosedur *Unique Challenge Procedure* dimana *base station* mengenerate nilai 24-bit *value* dan mentransmisikannya ke *mobile station* di *Authentication Challenge Message.*
2. Perbedaan mendasar dari teknologi CDMA adalah sistem modulasinya. Modulasi CDMA merupakan kombinasi FDMA (Frekuensi Division Multiple Access) dan TDMA (Time Division Multiple Access). Pada teknologi FDMA, 1 kanal frekuensi melayani 1 sirkuit pada satu waktu, sedangkan pada TDMA, 1 kanal frekuensi dipakai oleh beberapa pengguna dengan cara slot waktu yang berbeda. Pada CDMA beberapa pengguna bisa dilayani pada waktu bersamaan dan frekuensi yang sama, dimana pembedaan satu dengan lainnya ada pada sistem coding-nya, sehingga penggunaan spektrum frekuensinya teknologi CDMA sangat efisien.
3. Enkripsi pada jaringan GSM menggunakan algoritma A3, A5 dan A8 sedangkan pada CDMA menggunakan algoritma Algoritma Rijndael.
4. Banyak kemungkinan untuk melakukan serangan pada sistem keamanan GSM, serangan itu dapat dilakukan pada algoritma A3, A5 maupun A8.
5. Jaringan CDMA memiliki tingkat keamanan yang lebih baik jika dibandingkan jaringan GSM, hal ini disebabkan karena sistem CDMA

menggunakan metode multiple division dengan code, dimana sinyal data ditumpangkan pada sinyal derau yang tersebar.

6. Jaringan CDMA menggunakan algoritma enkripsi Rijndael (*Rijndael Encryption Algorithm)* yang aman dan sangat cepat dan hanya memungkinkan penggunaan ukuran kunci 128, 192 and 256-bit.

7. Teknologi CDMA membuat kesulitan terhadap kegiatan penyadapan, baik yang bersifat terus menerus maupun sesaat karena mengimplementasikan 42-bit PN (*Pseudo-Random Noise*) sekuens yang disebut dengan "*Long Code"*.

8. Baik jaringan CDMA maupun jaringan GSM meskipun sistem keamanan telah diperbaiki dengan sempurna , tetapi masih ada peluang untuk melakukan penyadapan yaitu dengan melakukan skenario *sosial engineering*, yaitu dengan dapat berpura-pura sebagai pegawai operator maupun menyadap panggilan pada jaringan *backbone* operator.

DAFTAR PUSTAKA

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

[2] Golic J. Dr. , Cryptanalysis of Alleged A5 Sream Cipher, *http://jya.com/a5-hack.htm*, tanggal akses 20 November 2006.

[3] Pesonen Lauri, GSM Interception, *http://www.net-security.sk/telekom/phreak/radiophone/gsm/gsm-secur/netsec .htm, tanggal akses 20 November 2006l*

[4] Anonim, GSM Cell phones Cloned, *http://jya.com/gsm-clones.htm*, tanggal akses 20 November 2006

[5] Anonim, GSM Cloning, *http://www.isaac.cs.berkeley.edu/isaac/gsm-faq-html*, tanggal akses 20 November 2006

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

[7] Anonim, Teknologi Keamanan Pada Sistem cdma, *http://www.ristishop.com/artikel/portal_article_detail.php.htm*, tanggal akses 20 November 2006.

[8] Christopher Wingert and Mullaguru Naidu, CDMA 1XRT Security overview (e-book), WhitePaper, August 2004. Didownload dari, *http://3gpp.org*, 20 November 2006

[9] Anonim, CDMA End-to-End Security (e-book) , Nortel Network, 2005.