

**PEMBAHASAN MENGENAI  
GSM,GPRS,CDMA,3G,4G,HSDPA,EDGE dan DIAL UP**

Disusun untuk memenuhi salah satu tugas mata kuliah Komunikasi Data



Disusun oleh  
Ahmad Soleh Afif (D1A.07.0207)

JURUSAN SISTEM INFORMASI  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS SUBANG  
Jalan R.A Kartini Km.3 Telp. (0260) 411415 Fax.(0260) 415677

Januari 2009

## DAFTAR ISI

Halaman Judul .....	1
Daftar Isi.....	2
Kata Pengantar.....	3
BAB 1 Pendahuluan.....	4-5
BAB 2 Pembahasan	
2.1. GSM.....	6
2.1.1. Arsitektur GSM.....	6-7
2.1.2. Layanan Sistem Keamanan GSM.....	7-8
2.1.3. Mekanisme Sistem Keamanan GSM.....	8-9
2.1.4. Jenis-jenis serangan GSM.....	10-12
2.2. CDMA (Code Division Multiple Access).....	13
2.2.1. Aspek Keamanan yang disediakan CDMA.....	13-15
2.2.2. Keunggulan Teknologi CDMA.....	16
2.3. EDGE (Enhanced Data Rates for GSM Evolution).....	16-17
2.4. GPRS (General Packet Radio Service).....	18
2.4.1. Arsitektur Umum Jaringan GPRS.....	18-19
2.4.2. Keamanan Jaringan GPRS.....	19-20
2.4.3. Penyerang.....	20
2.5. HSDPA (High Speed Downlink Packet Access).....	20-21
2.6. 3G (Third Generation).....	21-24
2.7. 4G (Fourth Generation).....	24
2.7.1. Keunggulan 4G.....	24
2.8. PSTN .....	24-26
BAB 3 Kesimpulan.....	27
Daftar Pustaka.....	28

## KATA PENGANTAR

Puji dan syukur penulis haturkan kepada Allah Swt yang telah memberi rahmat dan hidayahnya sehingga penulis dapat menyelesaikan tugas pembuatan makalah ini sembari juga menyampaikan salam kepada Nabiyallah Muhammad Saw yang syafa'atnya kita harapkan di hari akhir.

Penulis menyusun makalah ini dengan tujuan untuk memenuhi salah satu tugas mata kuliah Komunikasi Data dan juga penyusun mengharapkan agar makalah ini dapat bermanfaat dan menambah pengetahuan bagi penulis secara khusus juga kepada para pembaca secara umum.

Penulis ingin mengucapkan terima kasih kepada berbagai pihak yang telah membantu dalam penyelesaian makalah ini, diantaranya kepada Bapak Achmad Syafa'at yang telah membimbing penulis dalam mata kuliah Komunikasi Data juga kepada kedua orang tuaku yang telah mendukung dalam bidang materil maupun yang lainnya juga kepada pihak yang telah membantu dalam pembuatan makalah ini yang tidak penulis sebutkan satu persatu.

Akhirnya penulis menyadari makalah masih jauh dari kata baik, oleh karena itu penulis mengharapkan kritik dan saran yang membangun guna perbaikan di masa yang akan datang.

Subang, Januari 2009

Penulis,

## BAB 1 PENDAHULUAN

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 umumnya pada jaringan GSM digunakan algoritma A3, A5 dan A8. Enkripsi tersebut 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 kriptanalisis 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*.

*General Packet Radio Service* (GPRS) merupakan momentum penting bagi perkembangan teknologi seluler, di mana diperkenalkannya layanan paket data pada komunikasi seluler. Dengan dukungan terminal yang dilengkapi berbagai perangkat tambahan seperti kamera dan video, maka beberapa layanan multimedia dan aplikasi data dapat kita nikmati. Kehadiran teknologi *Code Division Multiple Access* (CDMA 2000 1X) disusul dengan kehadiran teknologi CDMA EV-DO akan meramaikan pertumbuhan komunikasi data. Di samping itu, platform *Global System for Mobile* (GSM) yang mendominasi 80% operator seluler di dunia dalam memenuhi kebutuhan akan *bandwidth* yang lebih besar, menjadi pendorong diperkenalkannya teknologi EDGE (*Enhanced Data rate for GSM Evolution*) yang akan mendukung layanan data dengan kecepatan 384 Kbps (*Kilobyte per second*). Dengan kehadiran teknologi EDGE dan CDMA EV-DO akan semakin memungkinkan adanya layanan data yang atraktif dengan akses data yang cepat. Layanan data akan mengalami pertumbuhan yang signifikan, baik dari sisi jumlah penggunaannya maupun variasi layanan yang dikonsumsi. Menurut perkiraan, penggunaan komunikasi data akan mempunyai porsi perbandingan: *voice* sebesar 40 persen dan data 60 persen. Layanan multimedia, di mana suara, data, dan video dapat diakses secara bersamaan dengan kecepatan data yang tinggi dan *bandwidth* yang besar yang disediakan EDGE, menjadi alasan utama untuk memperkenalkan generasi ke-3 (3G). Sejak tahun 2000, platform teknologi internasional GERAN (*GSM, EDGE Radio Access Network*) telah mengadopsi seluruh spesifikasi 3 GPP (*Third Generation Project Partnership*). Hal ini menjadikan teknologi EDGE masuk ke dalam kelompok teknologi yang memenuhi kualifikasi generasi ke-3. 3 GPP sebagai media standarisasi internasional membuka lebih banyak kemudahan untuk berkomunikasi tanpa ada keterbatasan baik dari segi tempat maupun waktu. Dukungan badan standarisasi internasional dan *open interface*, merupakan kunci sukses dari teknologi 3G dan aplikasinya. Implementasi EDGE pada jaringan GPRS yang ada akan membuat meningkatnya kapasitas, yang biayanya akan jauh lebih murah ketimbang membangun jaringan ber-*traffic* GPRS dengan tambahan lainnya. Maka perlu berhitung agar berbagai pilihan yang tersedia guna mencapai penerapan yang

terakhir yakni UMTS (*Universal Mobile Telecommunication System*). Layanan berbasis teknologi EDGE bisa memberikan hampir semua layanan generasi ke-3, yakni: *high quality, audio streaming, video streaming, online gaming, high speed download, high speed network connection*.

## BAB 2 PEMBAHASAN

### 2.1.GSM (Global System For Mobile Communication)

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.berdasar atas prinsip keamanan dengan Konsorsium GSM ketidakkennalan, maksudnya adalah algoritma enkripsi akan sulit di pecahkan jika algoritma tersebut tidak dipublikasi.

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. 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.

#### 2.1.1.ARSITEKTUR GSM

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

##### 1. Mobile Station (MS)

###### a. 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.

###### b. Subscriber Identify Module (SIM)

SIM adalah sebuah *smart card* yang mengidentifikasi 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.

## 2. Base Station Subsystem (BSS)

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

## 3. 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.

## 4. 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.

## 5. Visitor Locator 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.

### 2.1.2.Layanan Sistem Keamanan 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 Subscriber Identity*) yang unik tidak dalam bentuk plainteks (sudah terenkripsi).

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.

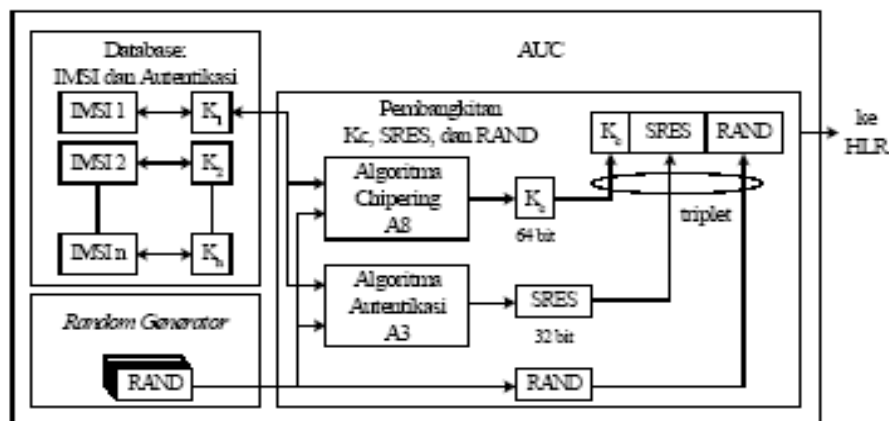
#### 1. Alokasi TMSI

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. Autentikasi

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

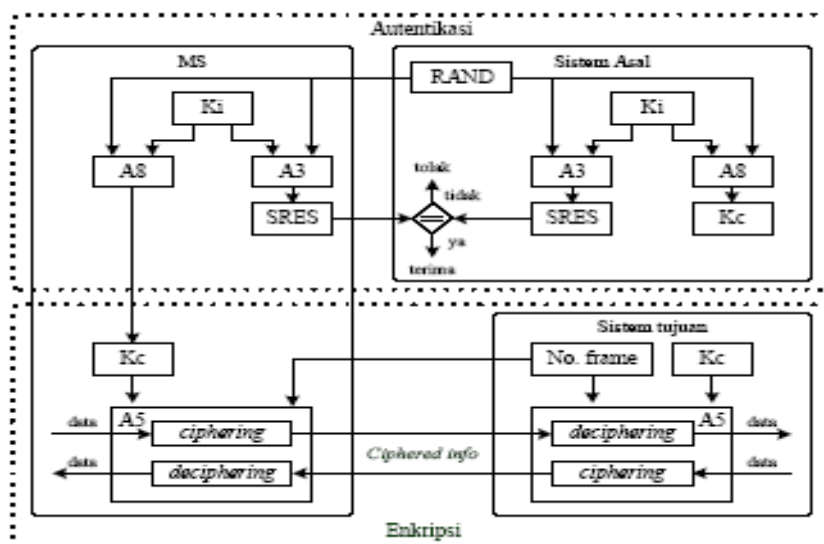
otentikasi dalam GSM dikenal dengan nama metoda *Challenge-Response*, yaitu teknik autentifikasi dengan cara memberikan *challenge* (RAND) kepada pelanggan untuk menghasilkan suatu informasi tertentu (*response*-SRES). Autentikasi tersebut melibatkan serangkaian parameter RAND, SRES, dan Kc yang disebut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



**Proses Pembangkitan Triplet**

### 3. 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.

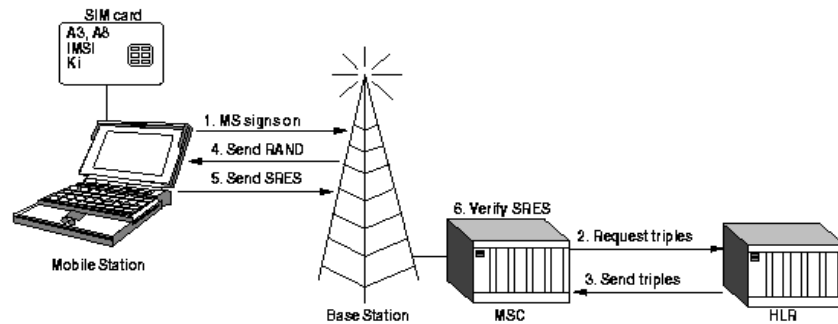


**Proses Autentifikasi dan Enkripsi**

#### 2.1.3. Mekanisme Sistem Keamanan GSM

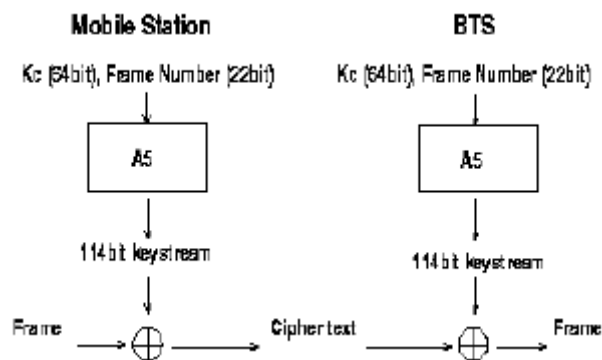
Sistem keamanan GSM berdasar pada pertukaran antara HLR ( Home Location Register) dengan kartu SIM pada MS (Mobile Station atau telepon selular). Data yang ditukarkan diatas yaitu Ki, yaitu kunci sepanjang 128 bit yang digunakan untuk membuat 32 bit response yang disebut SRES, sebagai jawaban dari adanya 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).

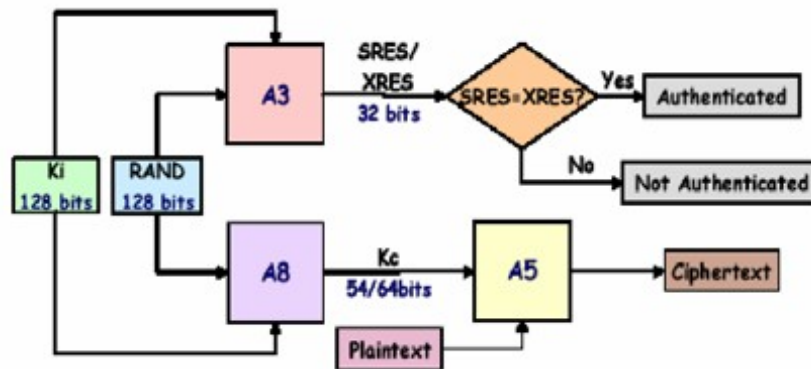


### Mekanisme Autentifikasi

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.



### Enkripsi dan Dekripsi Frame



Skema Algoritma GSM

#### 2.1.4. Jenis-jenis serangan pada GSM

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

##### 1. Serangan Brute Force pada A5

Serangan brute force secara *real-time* pada sistem keamanan GSM tidak relevan. Hal itu dikarenakan waktu kompleksitas untuk serangan ini sekitar  $2^{24}$  ( $2^{24}$  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 prosesor Pentium III dengan 20 juta transistor dan implementasi untuk satu set LFSRs (A5/1) membutuhkan 2000 transistor, maka kita akan memiliki 10.000 implementasi A/5 secara paralel dalam satu prosesor. 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 implementasi A5/1. Maka untuk jumlah kemungkinan kunci  $2^{24}$ , membutuhkan waktu sekitar 900.000 detik atau setara dengan 250 jam dengan satu prosesor. 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 multiprosesor, sehingga dapat mengurangi kebutuhan waktu secara drastis sebanding dengan banyaknya penggunaan prosesor.

##### 2. Serangan Divide and Conquer pada A5

Divide and Conquer yaitu serangan untuk mengurangi kompleksitas algoritma A5 dari  $2^{24}$  menjadi  $2^{24}$ , sehingga dapat mengurangi sebanyak  $29 = 512$  kali lebih cepat dari semula. Serangan divide and conquer berdasarkan pada known plaintext attack. Penyerang mencoba untuk mendapatkan inisial state dari LFSRs dari keystream yang diketahui. Penyerang ingin mengetahui semua nilai keystream bit sebanyak 64 bit. Nilai keystream itu dapat ditemukan jika penyerang mengetahui beberapa ciphertexts yang berkorespondensi dengan plaintexts. Ini bergantung pada besarnya format frame GSM yang dikirim kembali dan seterusnya. Frame GSM terdiri 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 plaintexts. Pada serangan divide and conquer diimplementasikan dengan menebak isi dari dua LFSRs yang pendek dan menghitung LFSRs yang ketiga dari nilai keystream yang diketahui. Ini dapat dilakukan dengan 2<sup>40</sup> serangan, jika clock dari dua register pertama tidak bergantung pada register yang ketiga. Karena nilai bit 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<sup>40</sup> menjadi 2<sup>45</sup>. J. Golub telah mengajukan divide and conquer yang lain berbasis asumsi yang sama dengan rata-rata kompleksitas dari  $2^{40.16}$ [2].

Golic menu Berdasarkan asumsi itu, dia menjelaskan bagaimana mendapatkan persamaan linear dengan menebak  $n$  bit pada LSFRs. Dengan menyelesaikan persamaan linear, 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. Objektif dari serangan ini untuk mendapatkan internal state dari tiga LSFRs pada waktu yang diketahui dan keystream sequence, kemudian merekonstruksi kunci sesi, Kc.

### 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 plaintext. 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 skenario lain jika penyerang menyerang 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 memungkinkan 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.

### 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 jika 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. 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 dianalisis. 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.

#### 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.

#### 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 autentikasi di MS. Prosedurnya sama dengan prosedur yang digunakan MS untuk mengakses kartu SIM. Perbedaannya adalah AuC lebih cepat dalam memproses permintaan 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.

#### 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 menghasilkan 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.

## 2.2.CDMA (Code Division Multiple Access)

CDMA (Code Division Multiple Acces) merupakan suatu menggunakan teknologi spread-spectrum untuk mengedarkan sinyal informasi yang melalui bandwidth yang lebar (1,25 MHz). Teknologi ini awalnya 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*”

### 2.2.1. 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 mengkonfirmasi 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 *subkey* yang disebut “*Shared Secret Data*” (SSD). *AKey*, *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

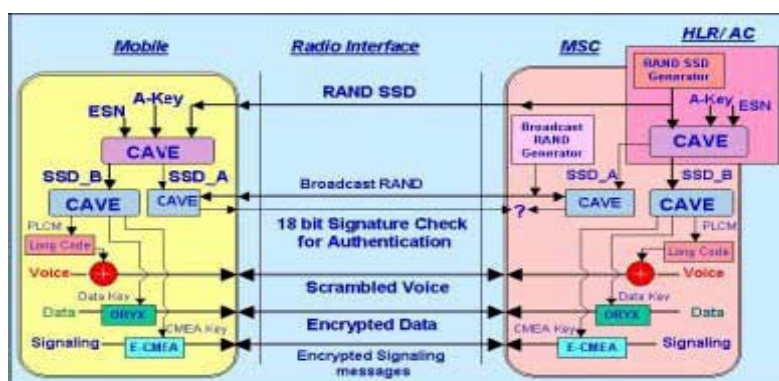
memungkinkan *local authentication*. SSD yang baru dapat digenerate ketika *mobile* kembali ke jaringan *home* atau *roam* ke sistem yang berbeda. Jaringan CDMA, *mobile* menggunakan SSD\_A dan broadcast RAND\* sebagai input terhadap algoritma CAVE untuk membangkitkan 18-bit *authentication signature* (*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 *authentication* 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. Akey 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 algoritma Diffie-Hellman key, *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 elegitimasi *subscriber*. Keamanan A-Key merupakan komponen terpenting dalam sistem CDMA.

### 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 sistem 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.



Ilustrasi Autentifikasi dan mekanisme enkripsi pada CDMA

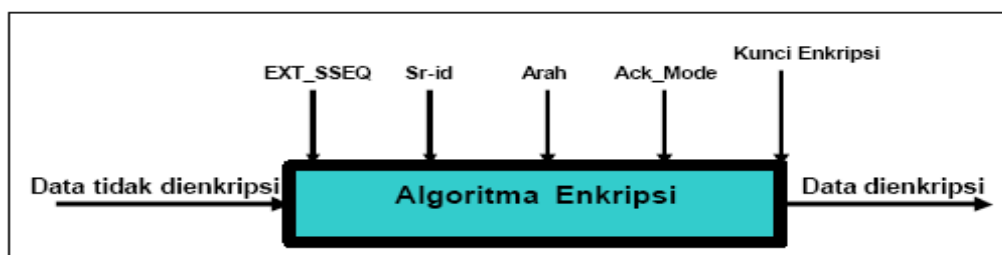
Desain semua telepon CDMA menggunakan kode PN (Pseudo-random Noise) yang unik untuk memperluas sinyal, yang mana hal ini membuat sinyal menjadi sulit untuk disadap.

### 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*. Algoritma 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.



Enkripsi dalam CDMA 1xEV-DV

Tabel 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 mode un-assured, dan yang lainnya di set "1"

### 2.2.2. Keunggulan Teknologi CDMA

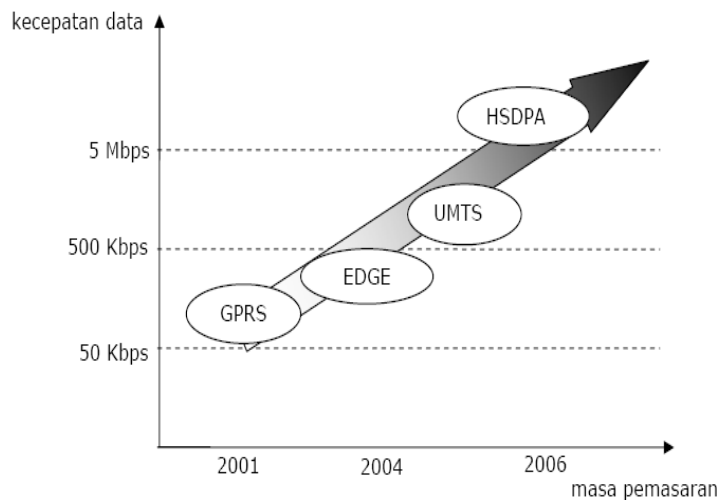
Teknologi CDMA memiliki keunggulan dalam beberapa hal, yaitu :

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 spread spectrum yang secara acak menyediakan bandwidth 1.250 KHz yang tersedia untuk masing-masing 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 bandwidth yang tersedia untuk pesan. Efisiensi 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 koordinasi 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 bandwidth 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 sistem
  - Memerlukan daya pancar yang lebih rendah, sehingga waktu bicara ponsel dapat lebih lama.
  - Mengurangi interferensi pada sistem lain.
  - Lebih tahan terhadap multipath.
  - Dapat dioperasikan bersamaan dengan teknologi lain (misal AMPS).

### 2.3. EDGE (Enhanced Data Rates for GSM Evolution)

EDGE adalah singkatan dari *Enhanced Data rate for GSM Evolution*, yaitu suatu sistem teknologi dari generasi ke-3 yang mempunyai kemampuan menghadirkan kecepatan transmisi data layaknya saluran *broadband* ke perangkat seluler (ponsel). EDGE juga diartikan sebagai *Enhanced Data rate for GSM/Global Evolution* yang merupakan cara peningkatan kualitas pada radio *interface* GSM yang sudah dibakukan. Dengan penerapan teknik EDGE akan diperoleh laju data yang semakin besar dan menghasilkan efisiensi pemakaian spektrum. Setelah teknologi GPRS (*General Packet Radio Service*), kini teknologi perseluleran nasional menuju implementasi EDGE pada jaringan GSM/GPRS. Pemanfaatan teknologi EDGE dengan menumpangkannya pada jaringan GSM/GPRS yang sudah ada membuat para pemakai dapat berkomunikasi lebih leluasa terutama komunikasi layanan data yang bergerak (*Mobile Data Service*) sebagai layanan seluler mutakhir, seperti: *high speed internet access, high speed network connection, full multimedia messaging, music clip, downloading video clip* dan *e-mail, high quality audio streaming, video streaming, dan online gaming*. Laju data yang ditawarkan EDGE adalah 3 kali lebih cepat dibandingkan laju data GSM/GPRS. Implementasi EDGE sempat mengalami masa keterlambatan, hal ini disebabkan oleh 2 hal. Hal pertama karena adanya anggapan bahwa penerapan UMTS (*Universal Mobile Telecommunication System*) dapat dilaksanakan tepat waktu, sehingga EDGE hanya dapat berperan pada *low traffic area* dan jenis layanan yang diberikan mirip dengan yang sudah disajikan UMTS. Hal kedua, penerapan UMTS mengalami keterlambatan. Akibat dari kedua

hal tersebut, maka pemanfaatan EDGE memang harus dilaksanakan. Ihtwal implementasinya teknologi EDGE dapat diterapkan pada *traffic* GPRS, maka ia disebut dengan predikat EGPRS (*Enhanced General Packet Radio Service*). Di samping itu, teknologi EDGE dapat berfungsi di dalam *traffic Circuit Switched Data* (CSD) yang disebut sebagai ECSD (*Enhanced Circuit Switched Data*). Teknologi EDGE hakikatnya dapat dipadukan ke dalam jaringan GSM yang sudah ada, apakah dengan memasang *transceiver* baru ataupun *base station* baru. Demikian juga EDGE dapat dikawinkan dengan jaringan TDMA (*Time Division Multiple Access*) dengan cara menambahkan *overlay* EGPRS secara lengkap. Sebenarnya, sejak awal 2004 jaringan telah berkemampuan teknologi EDGE yang mampu memberikan layanan data dengan kecepatan tinggi sampai 473,6 Kbps dalam kondisi konektivitas optimum, walaupun pada saat ini kecepatannya masih berkisar rata-rata 117 Kbps.



#### Kecepatan Data dengan Masa Pemasaran dari Tahun 2001 s.d. 2006

Kemampuan EDGE adalah 3–4 kali di atas rata-rata kecepatan akses jalur kabel telepon dan sekitar 2 kali lipat kecepatan CDMA 2000 1X. Layanan berkecepatan tinggi teknologi EDGE ini berjalan di lebar frekuensi 200 KHz GSM. Sebagai gambaran, CDMA 2000 1X kecepatan rata-ratanya hanya mencapai 70–80 Kbps dan maksimum 154 Kbps. Beragam ponsel yang akan ditawarkan yang dapat mengakses data dengan laju antara 118,4 Kbps – 400 Kbps, dapat dilihat berapa besar laju data tersebut bila dibandingkan jika kita mengaksesnya lewat komputer dan lewat jaringan telepon biasa, dengan cara *dial-up*, laju data yang diperoleh hanya berkisar 33 Kbps – 56 Kbps. Dengan teknologi EDGE serta pemanfaatan EGPRS akan dihasilkan efisiensi spektrum 2–3 kali lipat, sehingga tidak diperlukan penambahan perangkat *base station* dan *cell site*. EDGE merupakan salah satu standar untuk *wireless data* yang diimplementasikan pada jaringan seluler GSM, dan merupakan tahapan lanjutan dalam evolusi menuju *mobile multimedia communication*. Dengan EDGE, operator seluler dapat memberikan layanan komunikasi data dengan kecepatan lebih tinggi dibanding CSD (*Circuit Switched Data*) dan GPRS di mana CSD hanya mampu melakukan pengiriman data dengan kecepatan 9,6 Kbps dan GPRS berkemampuan sekitar 25 Kbps. Hadirnya teknologi EDGE yang memberikan layanan 3G merupakan teknologi telekomunikasi masa depan yang selalu mendominasi lahirnya inovasi layanan. Teknologi EDGE dari sudut pandang GSM adalah tahapan 2+ atau 2,5G sedangkan dari perspektif komunitas TDMA teknologi EDGE adalah perwujudan dari 3G. Evolusi GSM dari 2G ke 3G melalui GSM – GPRS – EDGE – WCDMA – HSDPA. EDGE adalah jalan tercepat untuk memiliki layanan 3G dengan menggunakan keberadaan spektrum. WCDMA (*Wideband Code Division Multiple Access*) dan HSDPA (*High Speed Downlink Packet Access*) memiliki efisiensi spektrum terbaik untuk *voice* dan data yang memiliki kecepatan data 384 Kbps–10 Mbps. Operator GSM memigrasikan jaringannya ke 3G dengan mempergunakan W-CDMA yang menggunakan *bandwidth* 5 MHz (*wideband*). W-CDMA mereplika protokol GSM agar tetap dapat menggunakan *core* jaringan GSM di jaringan generasi ke-3. Teknologi EDGE mempunyai kemampuan dengan laju yang

ditawarkan 3 kali lebih cepat dibandingkan laju data yang ditawarkan GSM/GPRS. Akses *packet downlink* kecepatan tinggi (*High Speed Downlink Packet Access* [HSDPA]) adalah layanan data berdasarkan paket dalam *downlink* W-CDMA (*Wideband – Code Division Multiple Access*) dengan transmisi data sampai dengan 8–10 Mbps.

#### **2.4.GPRS (General Packet Radio Service)**

GPRS yang termasuk dalam kelas 2.5 G adalah standard komunikasi data di jaringan GSM yang kecepatan transfernya mencapai 115 kbps. Dengan adanya GPRS ini jaringan GSM bisa memisah paket data kecepatan tinggi dengan suara. Dengan adanya GPRS ini pengguna bisa terus terkoneksi ke internet. Pengguna tidak perlu dial up terus menerus ketika akan melakukan koneksi ke internet. Tagihan internet tidak berdasar lama waktu penggunaan internet namun berdasar banyaknya data yang dikirim/diterima. GPRS menggunakan teknologi *packet switching* memungkinkan semua pengguna dalam sebuah sel dapat berbagi sumber-sumber yang sama; dengan kata lain para pelanggan menggunakan spektrum radio hanya ketika benar-benar mentransmisikan data. Efisiensi penggunaan spektrum pada akhirnya berarti kinerja yang lebih baik dan biaya yang lebih rendah. GPRS dapat menawarkan laju data sampai 115 kbps atau lebih. GPRS disebut teknologi 2.5 G karena merupakan langkah awal menuju teknologi transfer data kecepatan tinggi lewat jaringan nirkabel (3G). Sehingga sering disebut-sebut sebagai teknologi kunci untuk data bergerak. Secara rinci ada beberapa faktor yang menjadi pertimbangan bahwa GPRS merupakan teknologi kunci untuk data bergerak, yakni;

- mampu memanfaatkan kemampuan cakupan global yang dimiliki GSM (2G)
- memperkaya utiliti investasi untuk perangkat GSM yang sudah ada
- merupakan teknologi jembatan yang bagus menuju generasi ke 3
- berbasis paket data yang lebih efisien dalam penggunaan sumber daya
- memiliki laju data sampai 115 kbps yang berarti dua kali lipat daripada koneksi 'dial up' 56 kbps yang berlaku

Dengan adanya GPRS ini operator GSM dapat menambah layanan bagi para pengguna. Pengguna tidak hanya bisa melakukan komunikasi suara namun juga bisa melakukan komunikasi data. Beberapa layanan yang berkembang dengan adanya jaringan GPRS ini antara lain:

**MMS** (*Multimedia Messaging System*), dengan MMS ini pengguna bisa mengirimkan pesan dalam bentuk multimedia (suara, klip video, gambar)

**Traffic Monitoring**, dengan layanan ini pengguna bisa melihat keadaan lalu lintas di suatu tempat secara *real time*, dengan maksud agar mengetahui daerah mana yang macet dan daerah mana yang lalu lintasnya sepi.

**VOIP** (*Voice Over IP*), layanan ini biasanya digunakan antar pengguna PDA. Pemakai PDA pertama harus menginstal suatu program terlebih dahulu baru bisa menggunakan VOIP. Teknologi ini akan efektif bila tarif GPRS dihitung secara *flat*, sehingga walaupun banyak data yang ditransfer namun harga yang dibayarkan tetap sama.

GPRS dibagi menjadi 3 kelas berdasarkan kemampuannya, yaitu:

##### 1.Kelas A

Dapat dihubungkan ke jaringan GPRS dan GSM (suara dan SMS) pada waktu bersamaan penggunaannya, perangkat yang mendukung kelas A masih tersedia sampai saat ini.

##### 2.Kelas B

Dapat dihubungkan ke jaringan GPRS dan GSM (suara dan SMS) tetapi hanya satu yang dapat digunakan pada waktu yang sama. Ketika layanan GSM (telepon atau SMS) digunakan, maka GPRS harus menunggu dan akan otomatis aktif kembali setelah layanan GSM (telepon atau SMS) diakhiri. Kebanyakan perangkat GPRS termasuk dalam kelas B.

##### 3.Kelas C

Untuk menghubungkan layanan GPRS atau GSM (suara dan SMS), harus dilakukan pengantian layanan secara manual antara kedua layanan (hampir sama seperti kelas B hanya pengantian jaringan yang aktif tidak otomatis).

#### **2.4.1.Arsitektur Umum Jaringan GPRS**

##### 1. *MS – Mobile Station*

MS dapat dikatakan perangkat selular yang terhubung langsung dengan jaringan GSM, yaitu *SIM (Subscriber Identify Module) Card* dan perangkat keras seperti telepon selular, PDA, perangkat komputer yang terhubung menggunakan jaringan GPRS.

**2. BSS – Base Station System**

BSS terdiri dari BTS (*Base Transceiver Station*) dan BSC (*Base Station Controller*). Di BSS sinyal radio dari BSS akan diterima oleh BTS dan selanjutnya diteruskan ke BSC. BSC menangani sinyal yang dikirimkan oleh beberapa BTS.

**3. HLR – Home Location Register**

HLR adalah database yang menyimpan data pengguna jaringan GPRS. Informasi yang disimpan dalam HLR misalnya APN (*Access Point Name*).

**4. VLR – Visitor Location Register**

VLR adalah database yang berisi informasi semua MS yang sedang terhubung dengan GPRS.

**5. SGSN – Serving GPRS Support Node**

SGSN adalah komponen utama jaringan GPRS. SGSN akan meneruskan paket data dari/ke MS.

**6. GGSN – Gateway GPRS Support**

GGSN juga merupakan komponen utama jaringan GPRS. GGSN mengubah paket data GSM dari SGSN menjadi paket TCP/IP. GGSN dan SGSN digunakan sebagai penghitung pembayaran pemakaian internet.

**7. EIR – Equipment Identity Register**

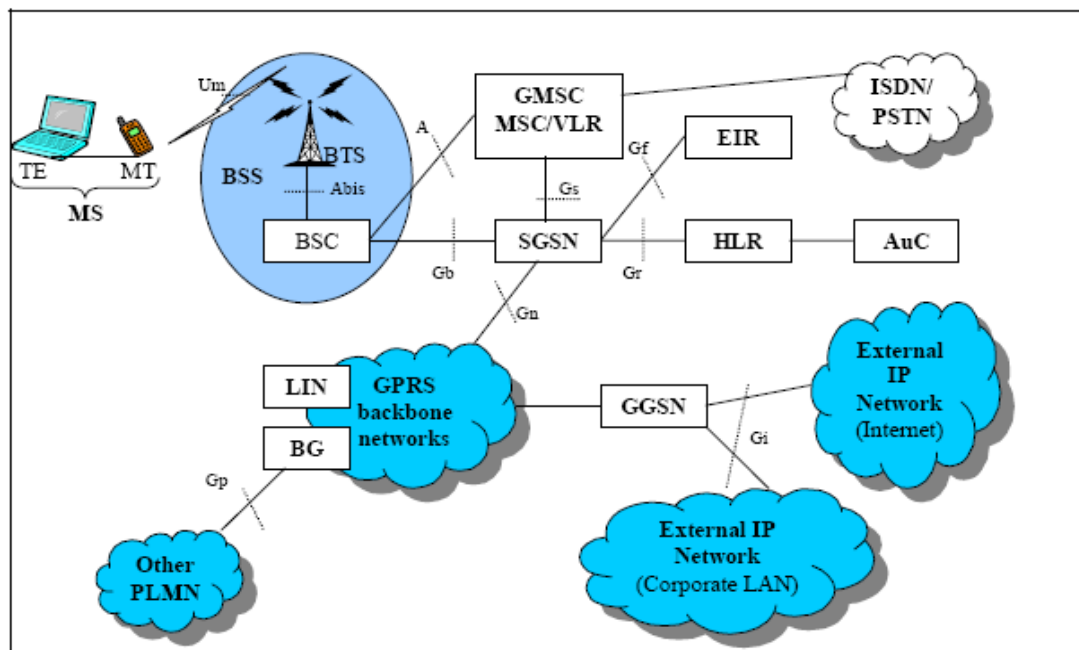
EIR adalah database yang berisi data tentang perangkat bergerak. Dalam EIR bisa berisi data-data IMEI dari telepon selular yang diperbolehkan/tidak diperbolehkan memakai GPRS.

**8. AuC – Authentication Center**

AuC adalah database yang berisi informasi pengguna yang diperbolehkan memakai jaringan GPRS. AuC merupakan bagian dari HLR.

**9. GPRS backbone networks**

GPRS backbone network adalah intranet dari jaringan GPRS. GPRS backbone networks adalah *IP based*.



**Arsitektur Jaringan GPRS**

**2.4.2.Keamanan Jaringan GPRS**

Dalam membahas mengenai masalah keamanan dalam suatu jaringan ada 3 topik utama yang harus diperhatikan. Topik bahasan tersebut adalah *confidentiality, integrity* dan *availability*.

- *Confidentiality*, berarti data-data dalam jaringan harus aman dari tantangan yang tidak berhak. Untuk menjaga data agar bisa memenuhi target *confidentiality*, data sebelum ditransmisikan dalam jaringan dienkripsi terlebih dahulu.
- *Integrity*, berarti data-data yang melewati jaringan harus tetap dalam keadaan utuh dan mengandung informasi yang sesungguhnya seperti pada saat dikirimkan. Data tidak boleh rusak di tengah jalan, sehingga untuk menjaga agar data tidak hilang/rusak harus ada *error checking* terlebih dahulu, baik pada saat/setelah melakukan enkripsi data, pada saat/setelah melakukan transfer data.
- *Availability*, berarti data-data dalam jaringan harus bisa diakses oleh yang berhak tanpa tenggang waktu. Data tidak boleh terlambat atau malah tidak dapat diakses sama sekali. Khusus untuk jaringan GPRS, dalam menjabarkan topik bahasan keamanan jaringan diatas, bisa dijabarkan dalam beberapa sub bahasan. Sub bahasan pertama adalah siapa saja yang berpotensi untuk mengacaukan masalah keamanan (penyerang), selanjutnya teknik-teknik apa saja yang bisa dilakukan penyerang untuk mengacaukan keamanan. Sub bahasan yang utama adalah bagian mana saja dalam jaringan GPRS yang berpotensi untuk dikacaukan.

### 2.4.3. Penyerang

Ada dua kategori utama yang berpotensi untuk menjadi penyerang dalam keamanan jaringan GPRS. Kategori yang pertama adalah penyerang dari luar, penyerang ini berasal dari luar operator dan dari luar pengguna jaringan GPRS. Yang termasuk dalam kategori yang pertama ini antara lain:

- *Cracker*; *cracker* mengarah ke penyerang yang berasal dari jaringan di luar jaringan lokal GPRS, biasanya berasal dari jaringan Internet. *Cracker* ini biasanya mempunyai tujuan untuk merusak sistem, atau hanya sekedar pamer kemampuan teknis saja. Namun tidak jarang *cracker* ini mempunyai motif ekonomi dengan mencuri data-data dari jaringan GPRS dan menjualnya ke pihak lain.
- Sub Kontraktor; sub kontraktor adalah pihak ketiga yang biasanya dikontrak oleh pihak operator untuk memasang atau mengupgrade jaringan selular. Pihak ini biasanya tidak berniat untuk melakukan untuk melakukan kerusakan, namun bila pihak ini melakukan kekeledoran dalam melakukan pemasangan jaringan, bisa menyebabkan masalah keamanan yang cukup fatal. Sub kontraktor bisa menjadi penyerang yang sangat potensial, mereka mempunyai akses ke jaringan dan bisa saja mengambil data-data penting dari pihak operator dan menjualnya ke operator yang lain.
- Rekanan; rekanan ini adalah pihak ketiga yang menyediakan dukungan penuh agar jaringan GPRS berjalan dengan semestinya, seperti ISP (*Internet Service Provider*). ISP menyediakan akses jaringan lokal GPRS ke jaringan internet. Sama seperti sub kontraktor, pihak rekanan biasanya tidak berniat melakukan kerusakan namun karena rekanan memegang salah satu kunci jalannya jaringan GPRS, bisa saja mereka menjadi perusak yang potensial.
- Pihak Keamanan; pihak keamanan ini bisa dari pihak kepolisian atau pihak militer. Pihak keamanan ini bisa melakukan pencurian data secara diam-diam (menyadap) di jaringan GPRS dengan segala macam teknik. Pencurian ini biasanya berhubungan dengan operasi intelejen. Selain itu pihak keamanan sering melakukan *jamming* (mengacaukan sinyal GSM), sehingga sinyal GSM dalam area tertentu sinyalnya menghilang. Aksi *jamming* ini biasanya berlangsung pada saat arak-arakan orang penting di jalan-jalan protokol dengan alasan keamanan orang penting yang sedang diarak.

Kategori yang kedua adalah penyerang dari dalam jaringan GPRS itu sendiri. Penyerang ini bisa berasal dari sesama pengguna GPRS ataupun dari pihak operator GPRS sendiri. Dari pihak operator GPRS bisa berupa pekerja yang dengan sengaja membocorkan data-data ke pihak lain dengan motif tertentu (misalnya: ekonomi).

### 2.5. HSDPA (High Speed Downlink Packet Access)

**High-Speed Downlink Packet Access (HSDPA)** adalah sebuah **protokol telepon genggam** dan kadangkala disebut sebagai teknologi **3,5G**. Teknologi ini dikembangkan dari **WCDMA** sama seperti **EV-DO** mengembangkan **CDMA2000**. HSDPA memberikan jalur evolusi untuk jaringan Universal Mobile Telecommunications System (**UMTS**) yang akan dapat memberikan kapasitas data yang lebih besar (sampai 14,4 Mbit/detik arah turun). HSDPA merupakan evolusi dari standar **W-CDMA** dan dirancang untuk meningkatkan kecepatan transfer data 5x lebih tinggi. HSDPA memdefinisikan sebuah saluran W-CDMA

yang baru, yaitu high-speed downlink shared channel (HS-DSCH) yang cara operasinya berbeda dengan saluran W-CDMA yang ada sekarang, tetapi hanya digunakan dalam komunikasi arah bawah menuju telepon genggam. Layanan HSDPA (high speed downlink packet access) menawarkan akses seluler dengan kecepatan sepuluh kali lipat dari jaringan 3G. Belum lenyap gegap-gempitanya peluncuran layanan 3G, kini para operator pemilik lisensi 3G mulai mengkampanyekan layanan 3,5 G, yang mereka sebut dengan layanan high speed downlink packet access (HSDPA). Sama-sama membutuhkan ponsel khusus, kedua layanan itu memiliki perbedaan yang menyolok dalam hal kecepatan aksesnya. Akses data melalui jaringan 3G hanya mampu menyediakan kecepatan maksimal 384 kilobite per second (kbps). Sementara, layanan HSDPA menawarkan akses dengan kecepatan hampir sepuluh kali lipat dari 3G, yaitu hingga 3,6 megabit per second (mbps).

## 2.6. 3G (Third Generation)

Teknologi 3G adalah teknologi komunikasi generasi ketiga yang menjadi standar teknologi telepon bergerak (mobile phone), menggantikan 2.5G. Hal ini berdasarkan ITU (International Telecommunication Union) dengan standar IMT-2000. Jaringan 3G memungkinkan operator jaringan untuk menawarkan jangkauan yang lebih luas dari fasilitas tingkat lanjut ketika mencapai kapasitas jaringan yang lebih besar melalui peningkatan efisiensi penggunaan spektrum. Kemampuannya meliputi komunikasi suara nirkabel dalam jangkauan area luas (wide-area wireless voice telephony), panggilan video (video calls), dan jalur data kecepatan tinggi nirkabel (broadband wireless data), dan semuanya itu berkerja dalam perangkat bergerak (mobile). Fasilitas tambahan juga meliputi transmisi data HSPA yang mampu untuk mengirim data dengan kecepatan sampai 14,4 Mbps untuk downlink dan 5,8 Mbps untuk uplink.

ITU mendefinisikan 3G sebagai teknologi yang:

1. Mempunyai kecepatan transfer data sebesar 144 Kbps pada pengguna yang bergerak dengan kecepatan 100 km/jam.
2. Mempunyai kecepatan transfer data sebesar 384 Kbps pada pengguna yang berjalan kaki.
3. Mempunyai kecepatan transfer data sebesar 2 Mbps pada pengguna diam (stasioner).

Teknologi 3G diperkenalkan pada awalnya adalah untuk tujuan sebagai berikut:

1. Menambah efisiensi dan kapasitas jaringan.
2. Menambah kemampuan jelajah (roaming).
3. Untuk mencapai kecepatan transfer data yang lebih tinggi.
4. Peningkatan kualitas layanan (QoS atau Quality of Service).
5. Mendukung kebutuhan internet bergerak (mobile internet).

Frekuensi yang digunakan oleh teknologi 3G, yaitu:

1. Frekuensi penerimaan (downlink) 1920-1980 MHz
2. Frekuensi pengiriman (uplink) 2110-2170 MHz

Yang termasuk teknologi 3G:

### **EDGE (Enhanced Data Rates for GSM Evolution) atau E-GPRS (Enhanced-General Packet Radio Services)**

Adalah teknologi 3G yang merupakan salah satu standar untuk wireless data yang diimplementasikan pada jaringan selular GSM. Diperkenalkan pertama kali pada tahun 2003 dan merupakan tahapan lanjutan dalam evolusi menuju mobile multimedia communication. EDGE awalnya disebut teknologi 2.75G. Namun sejak pertengahan tahun 2000, platform teknologi Internasional GERAN (GSM EDGE Radio Access Network) telah mengadopsi seluruh spesifikasi 3GPP (yang salah satunya adalah kecepatan transfer data sama dengan 3G) sehingga menjadikan teknologi EDGE masuk dalam kelompok teknologi generasi ketiga UMTS 3G. Dengan EDGE, operator selular dapat memberikan layanan komunikasi data dengan kecepatan lebih tinggi dibanding GPRS, di mana GPRS hanya mampu melakukan pengiriman data dengan kecepatan sekitar 25 Kbps. Begitu juga bila dibandingkan platform lain, kemampuan EDGE mencapai 3-4 kali kecepatan akses jalur kabel telepon (biasanya sekitar 30-40 Kbps) dan hampir 2 kali lipat kecepatan CDMA2000-1x yang hanya sekitar 70-80 Kbps. Kecepatan transfer data EDGE bahkan dapat mencapai kecepatan hingga 236,8 Kbps dengan menggunakan 4 timeslots dan 473,6 Kbps dengan menggunakan 8 timeslots.

Layanan berbasis teknologi EDGE berkemampuan memberikan berbagai aplikasi layanan generasi ketiga, yakni: high quality audio streaming, video streaming, online gaming, high speed download, high speed network connection, push to talk, dan lain-lain. Hingga bulan November 2006, EDGE telah diterapkan 156 jaringan operator GSM di 92 negara dan akan terus berkembang menjadi 213 jaringan operator GSM di 118 negara.

### **W-CDMA (Wideband-Coded Division Multiple Access) atau UMTS (Universal Mobile Telecommunication System)**

Adalah teknologi 3G yang dikembangkan di Eropa dan mulai diperkenalkan pada tahun 2004. Standarisasi dari UMTS ini dilakukan oleh ETSI (European Telecommunication Standard Institution), selain itu ITU-T (International Telecommunications Union Telecommunication Standardisation Sector) mengerjakan sistem yang sama dinamakan IMT 2000 (International Mobile Telecommunication System 2000). Kedua badan standarisasi ini dapat melakukan kerjasama sehingga terbentuk satu sistem untuk masa yang akan datang. UMTS dirancang sehingga dapat menyediakan bandwidth sebesar 2 Mbps. Layanan yang dapat diberikan UMTS diupayakan dapat memenuhi permintaan pemakai dimanapun berada, artinya UMTS diharapkan dapat melayani area yang seluas mungkin, jika tidak ada sel UMTS pada suatu daerah, maka dapat di-route-kan melalui satelit. UMTS dapat digunakan oleh perkantoran, rumah dan kendaraan. Layanan yang sama dapat diberikan untuk pemakai indoors dan outdoors, public areas, dan private areas, urban, dan rural. Frekuensi radio yang dialokasikan untuk UMTS adalah 1885-2025 MHz dan 2110-2200 MHz. Pita tersebut akan digunakan oleh sel yang kecil (pico cell) sehingga dapat memberikan kapasitas yang besar pada UMTS. Multiple access yang digunakan dapat mengalokasikan bandwidth secara dinamis sesuai dengan kebutuhan pelanggan. RACE (Research and Technology Development in Advanced Communications Technologies in Europe) telah mengembangkan dua jenis multiple access yakni CDMA dan TDMA, dari keduanya ini belum diputuskan yang akan digunakan. W-CDMA sudah di implementasikan di Jepang, Eropa, dan Asia, dan akan dikembangkan di 55 negara pada tahun 2006. Frekuensi UMTS berbagai daerah:

1. Asia dan Eropa (umumnya) pada frekuensi 2100 MHz (downlink) dan 1900 MHz (uplink)
2. Amerika Serikat (oleh operator AT&T Mobility) pada frekuensi 1900 MHz/850 MHz.
3. Amerika pada frekuensi 2100 MHz (downlink) 1700 MHz (uplink).
4. Eropa pada frekuensi 900 MHz.
5. Australia dan Jepang pada frekuensi 800 MHz.

### **CDMA2000-1x EV/DV (Evolution/Data/Voice) dan CDMA2000-1x EV-DO (Data Only/Data Optimized) atau IS-856**

Adalah teknologi 3G yang didukung oleh komunitas CDMA Amerika Utara, dipimpin oleh CDG (CDMA Development Group). CDMA2000-1x EV (Evolution) dan CDMA2000-1x EV-DO ini merupakan pengembangan dari teknologi CDMA2000-1x Release 0/RTT atau CDMA2000 (2.5G). Pada awalnya CDMA2000-1x EV-DO (Revision 0) hanya bisa mengirim data sampai 2,4 Mbps, tetapi kemudian berkembang sehingga CDMA2000-1x-EV-DO (data only) memiliki kecepatan seperti tabel di bawah.

**Tabel 2.7 Pembagian Kecepatan CDMA2000-1x**

	<b>Kecepatan</b>	<b>Aplikasi yang Didukung</b>
<b>CDMA2000-1x EV-DO Revision A</b> (T-1 2,45-3,1 Mbps speeds)		Video conference
<b>CDMA2000-1x DO Revision B</b>	EV-Rata-rata 300 Kbps, maksimal 73,5 Mbps	Transmisi data
<b>CDMA2000-1x DV</b>	EV-Rata-rata 300 Kbps, maksimal 3,09 Mbps	Integrasi layanan suara dan layanan multimedia data paket berkecepatan tinggi secara simultan
<b>CDMA2000-1x DO Revision C</b> atau kondisi	EV-Maksimal 280 Mbps pada puncak, 275 Mbps broadband	Voice over IP (VoIP), multimedia, informasi, entertainment, jasa

**UMB (Ultra Mobile Broadband)** downstream, 75 Mbps elektronik komersial, dan mendukung penuh jaringan jasa wireless pada lingkungan mobile (sehingga sama dengan jaringan Wi-Fi, WiMAX, dan UWB) upstream (sehingga dapat dikategorikan dalam 4G)

### **TD-CDMA (Time Division Code Division Multiple Access) atau UMTS-TDD (Universal Mobile Telecommunication System-Time Division Duplexing) di Eropa**

Adalah teknologi jaringan data 3G yang dibangun pada jaringan telepon selular standar UMTS/WCDMA di mana keduanya baik UMTS/WCDMA maupun TD-CDMA/UMTS-TDD tidak saling mendukung dikarenakan perbedaan cara kerja, desain, teknologi dan frekuensi yang dipakai. Di Eropa frekuensi yang dipakai UMTS-TDD ada pada 2010-2020 MHz yang dapat mentransfer data pada kecepatan 16 Mbps (saat kecepatan maksimum downlink dan uplink).

### **GAN (Generic Access Network) atau UMA (Unlicensed Mobile Access)**

Adalah teknologi 3G yang bertujuan agar sistem telekomunikasi dapat roaming dan dapat menangani jaringan LAN (WLAN) dan WAN dalam telepon selular secara bersamaan (diadopsi oleh 3GPP).

### **HSPA (High-Speed Packet Access)**

Adalah teknologi 3G yang merupakan teknologi dari penyatuan protokol teknologi mobile sebelumnya, sehingga memperluas dan menambah kemampuan (terutama dari sisi kecepatan transfer data) dari protokol UMTS yang telah ada sebelumnya. Karena adanya perbedaan kemampuan (downlink dan uplink) tersebut HSPA dibagi menjadi 2 standar, yaitu:

#### 1. HSDPA (High Speed Downlink Packet Access)

Merupakan standar HSPA dengan kemampuan dari sisi kecepatan transfer downlink-nya (dari jaringan ke handset), dimana HSDPA dapat mencapai kecepatan downlink 7.2 Mbps dan secara teori dapat ditingkatkan sampai kecepatan 14.4 Mbps dengan maksimum uplink 384 kbps. HSDPA selain dapat digunakan oleh handphone tetapi dapat pula digunakan oleh Notebook untuk mengakses data dengan kecepatan tinggi.

#### 2. HSUPA (High Speed Uplink Packet Access)

Merupakan standar HSPA dengan kemampuan dari sisi kecepatan transfer uplink-nya (dari handset ke jaringan), dimana HSUPA dapat mencapai kecepatan uplink secara teori sampai kecepatan 5.76 Mbps, tetapi HSUPA ini tidak implementasikan (dikomersialkan) dan handset-nya tidak dibuat.

### **HSPA+ (HSPA Evolution)**

Adalah teknologi 3G yang dikembangkan dari HSPA. Teknologi ini memiliki kecepatan transfer data sampai 42 Mbps pada downlink dan 11 Mbps pada uplink.

### **FOMA (Freedom of Mobile Multimedia Access)**

Adalah teknologi 3G pertama di dunia yang mengimplementasikan WCDMA. FOMA merupakan penamaan layanan 3G oleh operator NTT DoCoMo di Jepang.

### **HSOPA (High Speed OFDM Packet Access)**

Adalah teknologi 3G yang dikembangkan dari UMTS terutama pada teknologi antena yang menggunakan OFDM (Orthogonal Frequency Division Multiplexing) dan MIMO (Multiple-Input Multiple-Output). HSOPA dikenal juga sebagai Super 3G dapat mentransfer data sampai kecepatan 100 Mbps untuk downlink dan 50 Mbps untuk uplink.

### **TD-SCDMA (Time Division Synchronous Code Division Multiple Access)**

Adalah teknologi 3G yang masih dikembangkan Cina oleh CATT (Chinese Academy of Telecommunications Technology), Datang, dan Siemens AG atas proposal dari grup CWTS (China Wireless Telecommunication Standards) kepada ITU pada tahun 1999. Teknologi yang dikembangkan untuk menghilangkan ketergantungan pada teknologi barat, tetapi kurang banyak diminati para operator di Asia dikarenakan memerlukan peralatan yang benar-benar

baru dan tidak bisa menggunakan teknologi sebelumnya (CDMA2000-1x). TD-SCDMA menggunakan frekuensi 2010-2025 MHz, dengan kecepatan transfer data dari 9,6 Kbps sampai 2048 Kbps.

## **2.7. 4G (Fourth Generation)**

Teknologi 4G (juga dikenal sebagai Beyond 3G) adalah istilah dalam teknologi komunikasi yang digunakan untuk menjelaskan evolusi berikutnya dalam dunia komunikasi nirkabel. Menurut kelompok kerja 4G (4G working groups), infrastruktur dan terminal yang digunakan 4G akan mempunyai hampir semua standar yang telah diterapkan dari 2G sampai 3G. Sistem 4G juga akan bertindak sebagai platform terbuka di mana inovasi yang baru dapat berkembang. Teknologi 4G akan mampu untuk menyediakan Internet Protocol (IP) yang komprehensif di mana suara, data dan streamed multimedia dapat diberikan kepada para pengguna “kapan saja, di mana saja”, dan pada kecepatan transmisi data yang lebih tinggi dibanding generasi yang sebelumnya. Banyak perusahaan sudah mendefinisikan sendiri arti mengenai 4G untuk menyatakan bahwa mereka telah memiliki 4G, seperti percobaan peluncuran WiMAX, bahkan ada pula perusahaan lain yang mengatakan sudah membuat sistem prototipe yang disebut 4G. Walaupun mungkin beberapa teknologi yang didemonstrasikan sekarang ini dapat menjadi bagian dari 4G, sampai standar 4G telah didefinisikan, mustahil untuk perusahaan apapun sekarang ini dalam menyediakan kepastian solusi nirkabel yang bisa disebut jaringan seluler 4G yang tepat sesuai dengan standar internasional untuk 4G. Hal-hal seperti itulah yang mengacaukan statemen tentang “keberadaan” layanan 4G sehingga cenderung membingungkan investor dan analis industri nirkabel. Sebagian dari standar baku yang menyiapkan jalan bagi teknologi 4G meliputi:

### **UMTS Revision 8 atau 3GPP LTE (Third Generation Partnership Project Long Term Evolution)**

Adalah teknologi 4G yang masih dalam tahap pengembangan oleh 3GPP (Third Generation Partnership Project). Teknologi ini direncanakan untuk memiliki kecepatan rata-rata download 100 Mbps dan kecepatan rata-rata upload 50 Mbps, sehingga mendukung semua jaringan berbasis Internet Protocol (IP).

### **WiMAX (Worldwide Interoperability for Microwave Access)**

Adalah teknologi 4G yang mempunyai kemampuan transfer data jarak jauh secara nirkabel, juga point to point access untuk mendukung penuh akses telepon bergerak (mobile phone), sehingga dapat menjadi alternatif dari jaringan broadband dengan kabel dan DSL. Dalam aplikasinya WiMAX menggunakan frekuensi mulai dari 3,3 GHz, 3,5 GHz, 2,3 GHz, 2,5 GHz, atau 5 GHz (tergantung regulasi frekuensi tiap negara). WiMAX secara teori dapat mengirim data sampai kecepatan 70 Mbps dalam jarak 48 Km, namun dalam prakteknya WiMAX hanya mampu untuk mengirim data pada kecepatan 10 Mbps dalam jarak 10 Km untuk daerah bebas gangguan (pinggir kota) dan 10 Mbps dalam jarak 2 Km untuk daerah urban (perkotaan).

### **UMB (Ultra Mobile Broadband) atau CDMA2000-1x EV-DO Revision C**

#### **2.7.1. Kelebihan Teknologi 4G**

##### **Kelebihan**

Mendukung service multimedia interaktif, telekonferensi, wireless internet

Bandwidth yang besar untuk mendukung multimedia service

Bit rates lebih besar dari 3G

Global mobility (skalabilitas untuk jaringan mobile), service portability, low-cost service (biaya yang murah sampai 100 Mbps)

Sepenuhnya untuk jaringan packet-switched

Jaringan keamanan data yang kuat

## **2.8. PSTN**

Penggunaan telepon sebagai media komunikasi sudah umum dijumpai dalam masyarakat kita. Sebagai salah satu peranti elektronika telepon menggunakan sinyal

dengan frekwensi tertentu untuk berkirin pesan. Pada saat melakukan dial (menekan nomor tujuan) dan pada saat terjadi komunikasi maka sinyal di lewatkan media kabel telapon untukberkomunikasi antara dua pihak yang sedang berhubungan. Selain dapat digunakan untuk berkomunikasi antar manusia, telepon juga dapat digunakan untuk berkomunikasi antara manusia dengan alat elektronik. Salah satu contohnya adalah komunikasi jarak jauh antara manusia dengan peranti komputer. Atau komunikasi jarak jauh antara manusia dengan perangkat elektronik pengaman rumah. Telpon PSTN maupun handphone saat ini menggunakan sistem yang dikenal secara umum disebut DTMF yaitu dual tone multiple frequencys. Telephon PSTN pada umumnya memiliki 10 buah tombol ditambah \* dan # jadi jumlahnya adalah 12. sebenarnya disamping 12 angka dan simbol tersebut masih ada 4 huruf yang bisa kita letakan disana katakanlah A, B, C dan D. Jadi semuanya terdapat 16 tombol. Di dalam komunikasi ke enambelas tombol tersebut dikirimkan dengan 2 frekwensi yang berbeda. Satu frekwensi masuk ke dalam grup frekwensi tinggi dan satu frekwensi lagi masuk ke dalam grup frekwensi rendah. Masing masing grup memiliki 4 macam variasi (nilai frekwensi) sinyal sehingga dengan 2 grup fekwensi tadi dapat di kodekan 16 (4 pangkat 2) macam simbol. Untuk lebih jelas dapat dilihat pada tabel dibawah ini:

<b>Frekwensi Rendah (Low Frequencies)</b>		<b>1209 Hz</b>	<b>1336 Hz</b>	<b>1477 Hz</b>	<b>1633 Hz</b>
	<b>679 Hz</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>A</b>
	<b>770 Hz</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>B</b>
	<b>852 Hz</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>C</b>
	<b>941 Hz</b>	<b>*</b>	<b>0</b>	<b>#</b>	<b>D</b>

Tabel frekwensi DTMF

### Rangkaian DTMF Decoder

Untuk menangkap tombol apa yang ditekan oleh penelepon maka peranti pertama yang harus disediakan adalah peranti yang bertugas mendeteksi sinyal apa yang dikirimkan. Jika sinyal yang dikirimkan bukan sinyal bicara melainkan sinyal yang dikarenakan penekanan tombol telepon maka dapat digunakan tabel 1 untuk melakukan pendekode-an. Untuk itu diperlukan sebuah rangkaian elektronik yang mendapat masukan dari kabel telepon dan keluaran bilangan hasil pendekodean sinyal tersebut. Jika dilihat tombol tombol yang di kodekan ada 16 buah, digunakan 2 buah nada dengan variasi nilai masing masing nada 4 nilai. Keluaran dari rangkaian ini yang diharapkan adalah bilangan biner 4 digit. Dari tabel 1 dapat di buat tabel 2 dibawah ini yang menunjukkan konversi masukan menjadi keluaran. Karena ada 16 buah keluaran sebetulnya keluran ini jika dilambangkan dengan bilangan biner dapat diwakili dengan 4 bit bilangan biner dari 0000 sampai dengan 1111.

### Fungsi Transfer dari input menjadi output

Frekwensi rendah	Frekwensi Tinggi	Tombol yang ditekan
679 Hz	1209 Hz	1
679 Hz	1366 Hz	2
679 Hz	1477 Hz	3
679 Hz	1633 Hz	A
770 Hz	1209 Hz	4
770 Hz	1366 Hz	5
770 Hz	1477 Hz	6
770 Hz	1633 Hz	B
852 Hz	1209 Hz	7
852 Hz	1366 Hz	8
852 Hz	1477 Hz	9
852 Hz	1633 Hz	C
941 Hz	1209 Hz	*
941 Hz	1366 Hz	0
941 Hz	1477 Hz	#
941 Hz	1633 Hz	D

Untuk keperluan mendekode masukan tersebut diperlukan sebuah peranti elektronika dengan masukan sinyal telepon dan keluaran logika 4 bit. Untuk keperluan ini dapat digunakan salah satu produk IC Dual Tone Multiple Frequencies Dekoder yaitu MT8770 produk MITEL

## BAB 3

### 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.
9. Hadirnya teknologi EDGE yang memberikan layanan 3G, semakin menguatkan bahwa teknologi GSM yang digunakan oleh sekitar 80% negara di seluruh dunia ini merupakan teknologi telekomunikasi masa depan yang selalu mendominasi lahirnya inovasi layanan dibanding teknologi platform lainnya seperti CDMA.
10. Kecepatan data yang berjalan di platform EDGE maksimum bisa mencapai 478,3 Kbps dalam kondisi konektivitas optimum. Dengan kecepatan yang dimiliki EDGE, maka sangat memungkinkan memberikan layanan audiovisual yang sangat atraktif dan akses yang sangat cepat.
11. Melalui teknologi EDGE, dengan memanfaatkan EGPRS, akan dihasilkan efisiensi spektrum antara 2 sampai 3 kali lipat, yang berarti operator tidak memerlukan penambahan lagi perangkat *base station* dan *cell site*.
12. EDGE merupakan salah satu standar untuk *wireless data* yang diimplementasikan pada jaringan seluler GSM dan merupakan evolusi menuju *Mobile Multimedia Communication*.
13. Kecepatan data yang berjalan di platform EDGE lebih cepat dari CDMA.

### **Daftar Pustaka**

A.B. Carlson, "Communication Systems", McGraw-Hill Book.Co. 1968.

<http://jya.com/gsm-clones.htm>

[http://en.wikipedia.org/w/index.php?title=Mobile\\_radio\\_telephone&oldid=223930850](http://en.wikipedia.org/w/index.php?title=Mobile_radio_telephone&oldid=223930850).

<http://ilmukomputer.com/wp-content/uploads/2007/07/anjars-teknologi-3g.pdf>.

[http://www.rfidc.com/docs/introductiontomobility\\_standards.htm](http://www.rfidc.com/docs/introductiontomobility_standards.htm).