Secure GSM systems

با ظهور تلفنهای همراه دیجیتال این تصور نادرست بوجود آمد که این نسل جدید از استراق سمع در امان هستند. درصورتیکه این طور نیست، با اینکه شرایط تا حدی پیشرفت کرده است. موقعیتی که یک نفر می توانست مکالمه فرد دیگری که در کانال آنالوگ مجاور قرار داشت را در حالت عادی بشنود دیگر دلیلی برای نگرانی نیست.سیستم موبایل آنالوگ حقیقتاً امنیت خوبی نداشت ولی همانطور که خواهیم دید سیستم دیجیتال با وجود اینکه معماری با تکنولوژی بالاوشگفت انگیزی دارد،هنوز در معرض مهاجمهای جدی ای قرار دارند. در واقع سیستم جهانی ارتباط موبایل (GSM)طراحی شده تا همان سطح امنیت و قابلیت اعتماد را که در خطهای عمومی تلفنهای شبکه (PSTN) وجود دارد را ارایه دهد.

هیچ شکی در این نیست که سرویس GSM کیفیت صدای خیلی بالاتر، هزینه نهایی کمتر، سطح امنیت بالاتر ، سیر جهانی و انواع گوناگون امکانات و سرویسهای جدید را ارایه می دهد. برای دستیابی به درک بهتر از ضعفهای سیستمGSM ، این بخش به معرفی معماری پایه و اجزاء سیستم مورد بحث می پردازد.

۱ -۵ معماری پایه GSM

سیستمGSM یک سیستم سلولی است که اجهزه استفاده دوباره از طریق سازماندهی سهمیه اشان در الگویی خاص به نام خوشه را می دهد.(شکل۱ -۵) . سایز سلولها در این شکل مطابق با قدرت انتقال تغییر می کند ، در رنج ۲/۵تا ۳۲۰وات از ایستگاه محلی یعنی ایستگاه گیرنده/فرستنده اصلی . . (BTS).به این معنا که شکل و ا ندازه سلولها و خوشه ها مناسب برای وفق دادن نیازها و احتیاجات در یک شرایط خاص است. یک سلول بزرگ ممکن است حدود چندین کیلومتر باشد که تعداد کمی از تماسها را فراهم کند، در صورتیکه کوچکترین سلول ممکن است تراکم بالایی داشته باشد ، مثل فرودگاه که چندین کانال برای تماس در یک زمان مورد نیاز است. حتی تراکم بیشتر تماسها ممکن است نیاز به پوشش فقط یک ساختمان با یک ستوت را بوجود آورد . این سلولها میکرو سلول نامیده می شود و مرتبا استفاده می شوند تا توانایی سیستم در شهرهای بسیار شلوغ را بالا ببرند. وقتی که کاربران موبایل میان سلولهای همجوار حرکت می کنند، یک فرآیند پیچیده ای باید اجرا شود و این عملیات سر بار زیادی را به سیستم تحمیل می کند، مخصوصا مواقعیکه حرکت موبایلها در جاده و بزرگراهها باشد. برای حل این مشکل سلولهای چتری در سطح این راهها ایجاد شده اند.

BTS های اینگونه سلولها معمولا قدرت انتقال بالاتری نسبت به سلولهای معمولی دارند، و انتقال دادن به یک روال قابل پیش بینی برای مرکز سویچینگ می شود.

علاوه بر ساختار شبکه های محلی، اپراتور GSMباید اتصالات داخلی و امکان وصل کردن با PSTN را فراهم کند. واسط بین دو سیستم در رابطه با امنیت بسیارپر اهمیت است زیرا که GSM

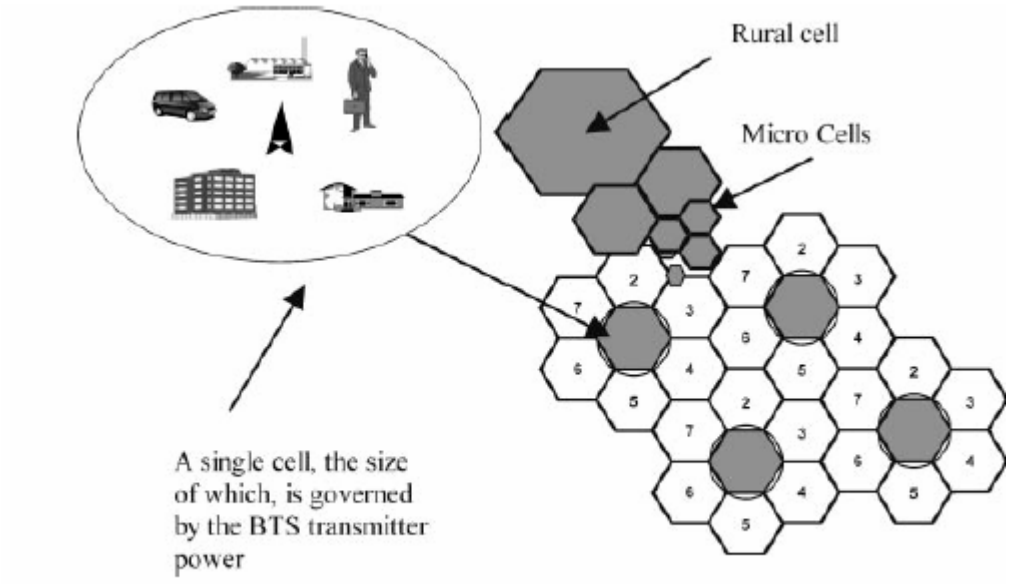

Figure 5.1 The cellular structure of the GSM system

یک مکانهایی که خالی از امنیت را دارد که ممکن است از آن پس در معرض آسیب قرارگیرند توسط تله های مرتبت با PSTN. چیزهایی که ممکن است در امنیت GSM قرار می گیرد، به طور حتم در سیستم تلفنهای عمومی اینطور نیست مگر اینکه پیشگیری های زیادی لازم باشد. تهیه کننده همچنین باید انتقالات و مدیریت مسیر یابی بین المللی مشتری ها را انجام دهد .این باعث بالا بردن امنیت هم می شود.

۱-۱-۵ اجزائ سیستم

- Mobile stations (handphone or car phone) (MS)
- Base transceiver station (BTS)
- Base station controller (BSC)
- Gateway mobile services switching center (GMSC)
- Operations & management center (OMC)
- Home location register (HLR)
- Visitor location register (VLR)
- Authentication center (AuC or AC)
- Equipment identity register (EIR)
- BTS-BSC interface (Abis)
- Air interface (Um)
- GSM algorithms A3 , A4 , A5 , A8

- Secret keys Ki &Kc

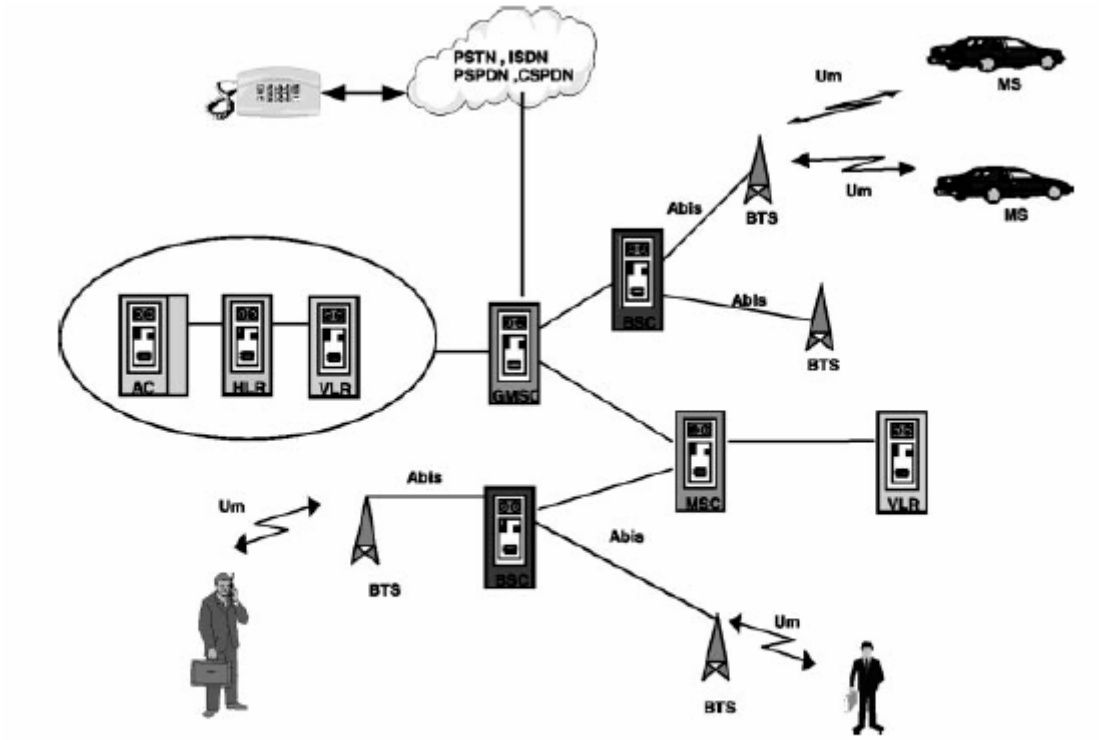

Figure 5.2 The interconnection of GSM system components

اتصالات بین این اجزاء و عملیات ضمنی آنها در شکل ۲- ۵به تصویر کشیده شده و در پاراگرافهای بعدی راجع به آن توضیح داده شده است.

MS: این یک تلفن شخصی یا تلفن ماشین با قدرت انتقال اطلاعات در رنج ۰/۸ ،۲،۵، ۸، ۲۰ وات می باشد. قدرت واقعی که برای برقراری ارتباط مورد استفاده قرار می گیرد ، طبق قرارداد با BTS متناظر است و از کمترین نیروی مناسب برای برقراری ارتباط استفاده می کند.

BTS: معمولا نزدیک مرکز سلول قرار می گیرد و قدرت خروجی آن از رنج چند صد متر تا چند کیلومتر است که انتخاب آن بستگی به سایز سلول دارد. هر BTS معمولا از ۱۶ فرکانس رادیویی (RF) کانالهای تلفنی تشکیل شده است.

BSC:ایستگاه مرکزی کنترل کننده است که BTS های مختلفی را کنترل می کند . بسته به سایزشبکه که کمتر از ۱۰ تا صدها BTS را برای کنترل در دست بگیرد.

GMSC:این واسط بین سلولی GSM,PSTN است ، GMSC مسیریابی تماسهایی که با شبکه GSM گرفته میشود یا تماسهایی که از طرف شبکه GSM گرفته میشود را کنترل میکند و اطلاعاتی راجع به مکان مبایلهای شخصی MS را با خود دارد.

OMC: نظارت سیستم بر پیغامهای خطا و موقعیت اجزاء شبکه گزارش میشود را بر عهده دارد. BTS , BSC ها را پیکر بندی میکند و کنترلی هم بر روی بار ترافیکی این واحدها دارد .

HLR:شامل تمام جزئیات کاربران در ناحیه متناظر با GMSC می شود. یکی از اجزاء اساسی امنیت IMSI, GSM (شماره بین المللی مشترکین موبایل) که در HLR ذخیره شده است که همراه کلید اعتبار سنجی ، شماره تلفن و جزئیات صورت حساب است . این یک مرکز برای کنترل امنیت است که بسیار با اهمیت است .

VLR: نقش بسیار مهمی را در عملکرد امنیت GSM بازی میکند . جزئیات مربوط به مبایل هایی که در منطقه متناظر با GMSC قرار دارند را در خود نگه می دارد ، از جمله TIMSI (خصوصیات موقت مشترکین موبایل) که در روند اعتبار سنجی کاربران مورد استفاده قرار می گیرد . همچنین جزئیات مکان های موبایلها در تا امکان GSMC را فراهم می کند مسیر یابی تماسها را بر قرار سازد .

AuC: کار اصلی اش این است که الگوریتم هایی را برای اعتبار سنجی در ایستگاه موبایل در GSM در خود جای می دهد بنا بر این یک فاکتور مهم در عملکرد امنیت GSM است و از دست رسی غیر قانونی و تجاوز به ان محافظت شده است .

EIR: جزئیات را شامل می شود ، مانند : شماره سریال تمام موبایل های گم شده یا به سرقت رفته که باید از استفاده انها از سیستم جلوگیری شود. تمام کاربران به رنگ سیاه یعنی کاربران غیر معتبر ، سفید یعنی مشترکین حقیقی و طوسی یعنی مشترکینی که مورد ظن هستند ویا تحت نظر می باشند، لیست می شوند .

Um : هوای است که واسط بین BTS , MS می باشد .

Abis : واسط بین BSC,BTS می باشد.

۲-۱- ۵ زیر سیستم GSM

اجزاء شبکه به ۳ زیر سیستم سازماندهی می شوند : ایستگاه موبایل ، ایستگاه اصلی زیر سیستم و شبکه زیر سیستم . (شکل ۳-۵)
MS شامل موبایل یا ترمینال همراه یک سیم کارت هوشمند است .دسترسی به سیم کارت توسط یک رمز عبور یا PINحفاظت شده که این PIN معمولا از شش عدد تشکیل شده که اگر سه بار رمز اشتباه وارد شود ، دیگر اجازه ورود نمی دهد و کارت بلاک می شود ، در نتیجه برقراری ارتباط با سیم کارت غیر ممکن می شود . سیم کارت می تواند انواع اطلاعات ، جدای از حافظه گوشی را در خود جای دهد. سیم کارت IMSI را نیز شامل می شود که برای شناسایی کاربران به سیستم مورد استفاده قرار می گیرد . خود سیم کارت نیز قابل حرکت است ، یعنی که کاربر می تواند آنرا وارد هر دستگاه تلفن دستی سازگار قرار دهد و از سیستم استفاده کند . سیم کارت و بویژه IMSIتا حدی در پروتکل امنیت GSM شرکت دارد که شامل کلید محرمانه برای اعتبار سنجی کاربران می باشد . MS همچنین الگوریتم A5 را هم شامل می شود که برای رمز گذاری تماسها در واسط Um استفاده می شود.
ایستگاه اصلی زیر سیستم شامل دو جزء مهم می شود:
* ارتباط BSC,BTS از طریق واسط Abis صورت می گیرد. BTS تا RF۱۶ فرستنده ، گیرنده برای سلولهایش حمل می کند و بنابراین سیگنال دهی بین MSو خودش را از طریق "هوا" یا واسط Um انجام می دهد.
* BSC همانطور که از نامش می توان فهمید ، عنصر کنترل کننده زیر سیستم است و جوابگوی یک یا چندین BST است . تنظیم کانالهای RF ، انتشار طیف امواج فرکانسهای مشغول، تماسهای بین سلولها و مسیر یابی تماسهای موبایل به MSC در صورت نیاز را انجام می دهد. یک تماس که در میان دو موبایل که در یک سلول قرار گرفته اند می تواند بوسیله BTS, BSC کنترل شود.
شبکه زیر سیستم شامل چهار جزء اصلی می شود :

- MSC
- VLR
- EIR
- AuC

- MSC : که موبایل مشابه مرکز سوئیچ PSTN می باشد و تماسها را به یا از طرف مشترکین

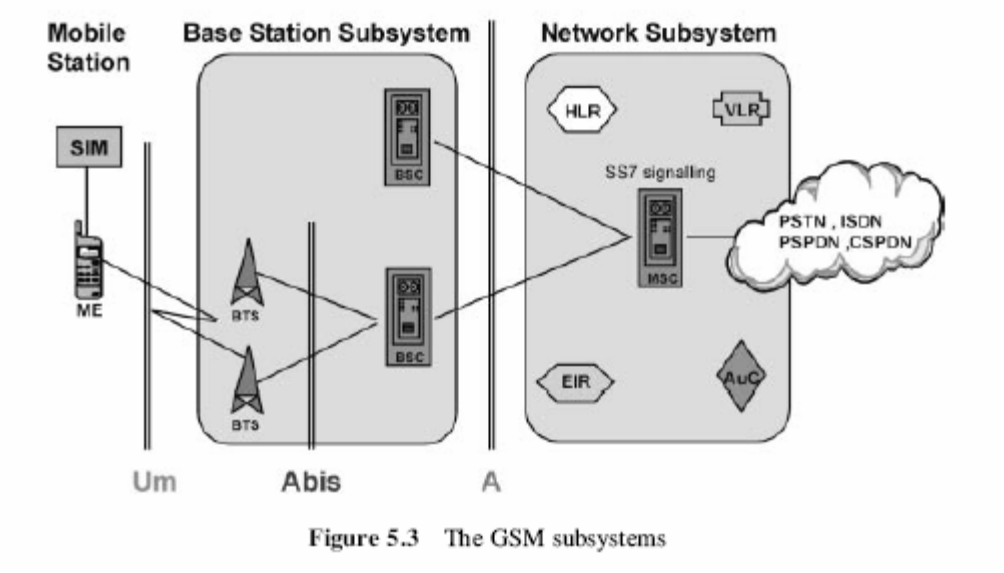

Figure 5.3 The GSM subsystems

موبایل وشبکه تلفنهای معمولی مسیر یابی می کند. MSC کنترل میکند که آیا IMSI و سیم کارت قرار است در پروتکل امنیت GSM شرکت کند یا نه، و MSC با ثباتهای مکانیابی ، EIR و AuC می توانند شریکهای اصلی در راهیابی باشند ، ثباتهای مکانیابی در جزئیات بیشتری در بخش ۵-۲-۱ بحث می شوند ولی در این لحظه میتوان به سادگی به عنوان تسهیل کننده مسیر یابی تماسها و عملیات سیر کردن ان را در نظر گرفت. همان طور که در بالا ذکر شد ، EIR یک پایگاه داده است که شامل لیستی از تمام تجهیزات موبایل که از شبکه استفاده می کند می باشد. هر موبایل با IMEI ی خودش شناسایی می شود و این شبکه را قادر میسازد تا بتواند بر کاربران خود نظارت داشته باشد و به کاربران معتبر خود اجازه دهد که از امکاناتش استفاده کنند، در حالیکه جلوی استفاده دستگاههای دزدیده شده یا تائید نشده را می گیرد. AuC یا مرکز اعتبار سنجی یک کارگاه داده حفاظت شده است که یک کپی از کلید های رمز گذاری که در عملیات اعتبار سنجی و رمز گذاری از طریق واسط Um استفاده می شود را در خود ذخیره می کند.

5.1.3 The GSM Radio Um Interface

باند GSM RF اصلی در باند 900Mhz دکل فرستنده قرار دارد ، به طور مثال از موبایل به BTS که بین 890 تا 915Mhz عملیات انجام میشود و از BTS به MS باند بین 935 تا 960Mhz استفاده می شود . با یک کانال که 200Khz پهنهی باند دارد، FDMA (تقسیم کننده فرکانس با چندین دسترسی) ۱۲۴ کانال برای تماسها با باندی بالای 25Mhz را می دهد. این بعدا به وسیله

TDMA (تقسیم کننده زمان با چندین دسترسی) گسترش پیدا میکند تا بتواند ۹۹۲ کانال حجیم دو طرفه برای مخابره تلفن را بدهد .
دیگر خصوصیات مهم کانالهای رادیویی شامل :

- الگوریتم سازگاری زمان که MS را قادر می سازد در یک مقطع زمانی تاخیر در انتشار را تصحیح کند .
- ماژول GMSK
- ارسال و در یافت گسسته که در بازه های زمانی خاصی ذر شرایط ارسال و دریافت از طرف MS خاموش می شودبا این تکنیک عملکرد باطری MS بهبود میابد و در ضمن تداخل کانالها کاهش میابد.
- FHSS یک تکنیک انتشار است که به محو سازی تداخلهای کانالها کمک می کند.این امکان وجود دارد که در بعضی مکانها مانند ساختمانهای بلند تداخل کانالهای رادیویی بوجود آید و یک سلول خاص مبتلا به کانالهای پر نویز دائمی شوند و کانالهای ضعیفی دهند.

ساختار استاندارد امنیت GSM

همانطور که قبلا ذکر شد ساختار استاندارد GSM شامل:

- The AuC
- HLR
- VLR
- SIM cards
- IMSI & TMSI
- Encryption
- TDMA
- Frequency hopping
- EIR/IMIE

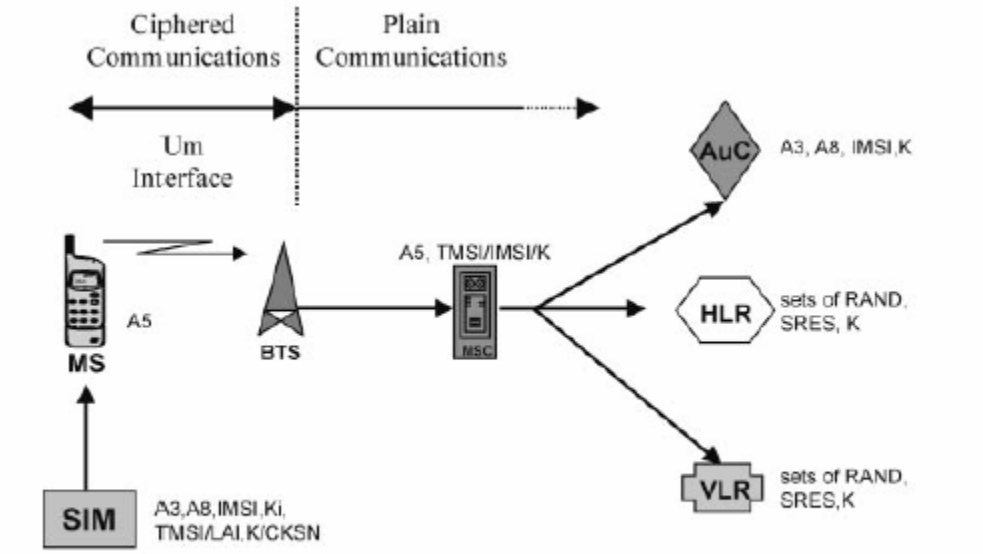

Figure 5.4 The distribution of GSM security elements

AuC : اعتبار سنجی پییغام و کاربر یک امر ضروری در امنیت ارتباطات می باشد. ولی این امر در مورد GSM صدق نمی کند ، زیرا که در تمام عملیات رادیویی دستگاه فرستنده گیرنده به صورت رایگان در دسترس هر گروه علاقمند به استفاده قرار می گیرد . مرکز اعتبار سنجی و واحدهای پشتیبان آن مثل HLR به سمت از بین بردن هر گونه تهدیدی به اعتبار سنجی میل می کنند. AuC چندین پارامتر را برای HLR فراهم می کند تا اعتبار سنجی یک کاربر موبایل را انجام دهد . AuC تمام الگوریتمهایی که از طرف شبکه در خواست می شود را با خود دارد و می داند که چه الگوریتمی را برای سنجش اعتبار یک مشتری خاص بکار ببرد . بنابر این AuCباید از سوء استفاده و حمله در امان باشد. سیم کارت هم الگوریتم کاربر خود را دارد و در ضمن AuCاعتبار سیم کارت کاربر را با استفاده از الگوریتم A3 که در سیم کارت و AuC ذخیره شده است چک می کند . که این کار را با استفاده از دو ورودی : یک کلید اعتبار سنجی (KI) ویک عدد تصادفی (RND) که 128BIT است انجام می دهد ، که بوسیله شبکه و از طریق واسط Um به موبایل ارسال می شود . این RND بوسیله MS ی که در حال گرفتن اعتبار است گرفته می شود تا RNDرا رمز گذاری کند و یک خروجی ایجاد می کند بنام SRES که 32BIT ای است . SRES دو باره به AuC فرستاده می شود تا دوباره چک شود که خطای محاسباتی نداشته باشد . طبق یک قرارداد MS را چک می کند که واجد شرایط باشد . هر کاربر غیر معتبری نمی تواند KI صحیح ویا الگوریتم A3 را داشته باشد و بنا بر این قادر به حساب کردن SRES صحیح نمی باشد. شماره تصادفی این اطمینان

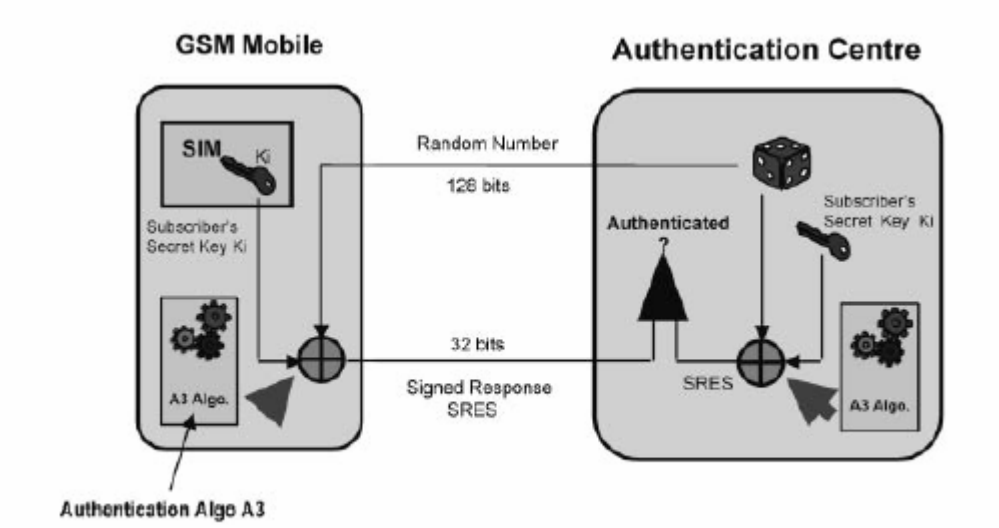

Figure 5.5 The GSM authentication process

را حاصل می کند که SRES در هر موقعیت وارد شدن به سیستم متفاوت است . این یک نوع مثال از سیستم سوال و جواب است.

HLR : هر شبکه GSMیک HLR داردکه یک تعدادی پارامتر حساس را در بر دارد ، از جمله جزئیات موبایل کاربر مثل صورت حساب ، الگوریتم A3 برای رمز گذاری پیغامها و رمز گذاری مشابه کلید Ki . HLR حتی می توا ند اعداد تصادفی مورد نیاز برای اعتبار سنجی را ایجاد کند .
از آنجائیکه HLR میزبان بسیاری از پارامتر های بحرانی می باشد ، هدف بسیاری از متجاوزان می باشد و باید از نحوه پنهانسازی خوبی برای امنیت استفاده کند تا از سوء استفاده در امان باشد .

VLR : شامل جزئیاتی از تمام موبایلهایی که در GMSC متناظر وجود دارد می با شد ضمن اینکه HLR تمام جزئیات مشترکان دائمی را دارد ، TMSI و IMSI مربوط به MS را هم دارد و برای سیگنال دهی Um استفاده می شود ، که باید از استراق سمع کنندگان در امان باشد . VLR همچنین موقعیت فیزیکی دقیق موبایل را به سیستم نشان می دهد و عملیات اعتبار سنجی در GMSC وقتیکه MS می خواهد برای اولین بار وارد یک شبکه دیگری شود را پشتیبانی می کند .

SIM Card : سیم کارت یا ماژول شناسایی کاربر یک کارت هوشمند یک پردازنده و تراشه حافظه دارد . سیم کارت قلب امنیت GSM می باشد ، که برای عملیات اعتبار سنجی و رمز گذاری سیگنالها

بسیار مهم است . این کارت شامل IMSI وهر دو الگوریتم A3 و A8 می باشد . بعلاوه سیم کارت کلید اعتبار سنجی شخصی ، Ki ، و عناصر کنترل کننده دسترسی اش ،PIN ، را در خود دارد . کنترل دسترسی به سیم کارت مبتنی بر مالکیت خود سیم کارت و اطلاعات شماره شناسایی شخصی می باشد . اگر شخصی PIN خود را فراموش کند یا کسی بخواهد دسترسی غیر مجاز به موبایل کسی داشته باشد اگر سه بار PIN را اشتباه وارد کند سیم کارت قفل می شود و سیم کارت قفل شده تنها با فراهم کردن و وارد کردن کلید شخصی باز کننده قفل (PUK) که هشت رقمی می باشد ، باز می شود . معمولا از مرکز سرویس دهنده که با یک مصاحبه شفاهی کاربر واقعی را تشخیص می دهد. جدا از پارامترهای امنیتی ، سیم کارت شامل جزئیات تماسهای شخصی مشترکین می باشد. مانند:

- شماره تلفن شخصی
- ID مشترک برای شبکه مثلIMSI
- حافظه پیغام کوتاه
- جزئیات برای امکانات مسیر یابی در طول سفرهای بین المللی
- جزئیات صورتحساب

جریان اطلاعات بین سیم کارت و VLR شبکه در شکل ۱۱-۵ نشان داده شده است .
با حرکت صنعت موبایل به سمت نسل سوم برای پشتیبانی از سیستمهای WAP و GPRS ، سیم کارتها برای عملیات پیچیده تر ی که از آنها خواسته می شود کافی نیستند .در ضمن ظرفیت حافظه داخل تلفن هم بدون شک ارتقاء پیدا می کند . سیم کارت هنوز برای پرداخت سرویسهایی از قبیل تجارت الکترونیک مورد استفاده قرار می گیرد . با توسعه شبکه های GPRS سیم کارت مشکلات امنیتی جدیدی پیدا می کند .نیاز به داشتن کارت دوم با قابلیت جابجایی که تنها می تواند داخل تلفن دستی شود در زمانیکه یک معامله تجارت الکترو نیکی صورت می گیرد ، احساس می شود .
در حال حاظر ، امنیت سیم کارت متکی به رمز گذاری متقارن است ، ولی در آینده که تکنولوژی تلفنهای موبایل پیشرفت کردند و سیم کارت قابلیت یک پارچه شدن با این پیشرفت را پیدا کرد ،سیم کارت اهمیت بیشتری را به عنوان وسیله ای برای اعتبار سنجی پیدا می کند . واضحترین جواب به این درخواست بکار بردن سیستم کلید عمومی است که هر دو کلید خصوصی و عمومی برای انجام مذاکره را دارد، لازم می باشد . کارت هو شمند یک وسیله ایده آل برای این کاربرد است .

IMSI & TMSI : TMSI برای مسیر یابی یک کاربر استفاده می شود بعد از اینکه عملیات اعتبار سنجی در رمز گذاری توسط VLR انجام شد . موبایل با تائید در خواست جواب می دهد . تمام عملیات بوسیله الگوریتم رمز گذاری A5 در امنیت قرار می گیرد . (شکل ۶-۵)
TMSI برای شناسایی اینکه مشترک در طول مدتی که در ناحیه ای با VLR خاص خودش قرار دارد و برای حفاظت از استراق سمع روی مسیرهای رادیویی بکار می رود . در طول مدتی که در آن ناحیه

قرار دارد می ماند و بر اساس پروتکل لحظه به لحظه عوض می شود و روی سیم کارت کاربر برای اتصال به شبکه در دفعات بعدی اش و در همان ناحیه می ماند . برای تماسهای خارج از ناحیه LAI لازم است که به همراه TMSI بیاید . بنابراین مشترکین اجازه دارند تماسهایی بر قرار کنند و موقعیت مکانی خود را عوض کنند بدون نیاز به اینکه IMSI مهم اشان اشاره کنند و بنابر این مکان مشترک مشخص نمی شود تا در دسترس هر گونه شنود از سیگنالهای موجود در واسط Um نباشد .

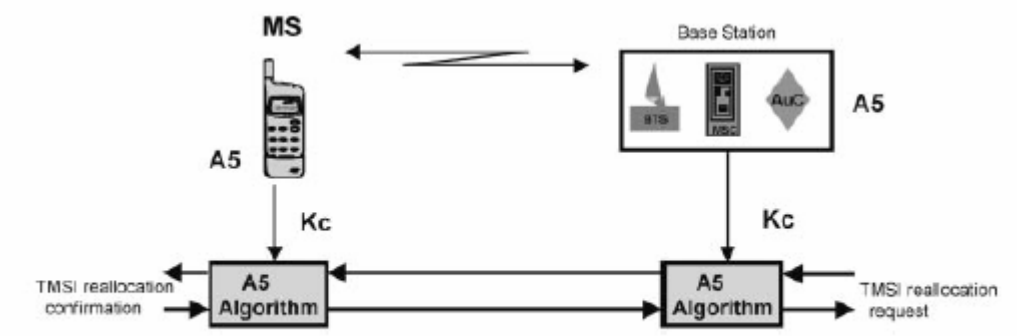

Figure 5.6 The TMSI application

رمزگذاری استاندارد GSM

کمی شک وجود دارد که سیستمGSM دارای امنیت خیلی بالا تری نسبت به رقیب سابق خود و مشترک همیشگی اش ، سیستم PSTN دارد . ماژول GMSK و TDMA برای از بین بردن استراق سمع مداوم بکار می روند . اما مشکل اصلی سیستم GSM از نظر امنیت همانطور که در شکل های۱۰-۵ و ۱۱-۵ با نشان دادن توسعه رمزگذاری سیگنالهای مسیر یابی اشاره شده ، این است که تنها قسمتی از انتقال GSM مه رمز گذاری می شود کانالهای رادیویی بین MS و BTS (به طور مثال واسط Um) هستند .باقیمانده مسیر سیگنال چه به مشترک تلفن ثابت یا به GSM دیگری که در سلول متفاوتی قرار دارد از سیستم تلفن عمومی عبور می کند ، جائیکه عموما هیچ حفاظت قابل اعتمادی وجود ندارد . بنابر این هر استراق سمع کننده ای نگرانی ای راجع به عوامل محافظت کننده ماندگار موجود در سیستم GSM ندارد به خاطر اینکه همه چیز به صورت ساده در عناصر BTS در شبکه قرار دارد . طبیعتا هر حمله کننده ای از ضعیفترین لینک استفاده می کند و اور گانیسمهای PSTN یا ISDN همینها هستند .

اشکال ۷-۵ و ۱۲-۵ که عملیات رمز گذاری صدا را نشان می دهند ملاحظه کنید .

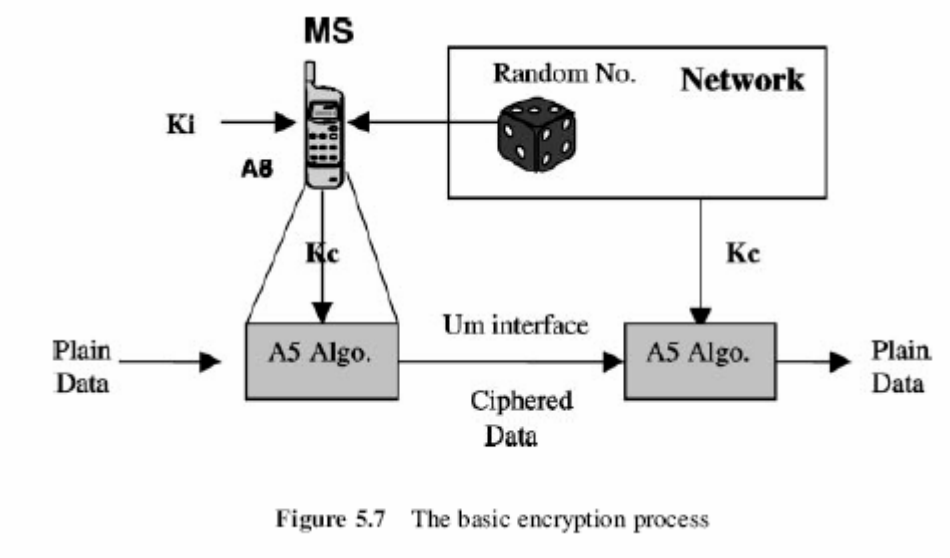

Figure 5.7 The basic encryption process

بلافاصله بعد از سیگنال SRES و اعتبار سنجی مشترک ، VLR به MSC دستور می دهد تا BSC و سپس BTS را کنترل کند داده Kc که از Ki و الگوریتم A8 در HLR نتیجه گیری شده از طریق BSC به BTS ارسال می شود ، در زمانی که BTS به موبایل (MS) دستور می دهد که به حالت رمز سوئیچ کند . MS یا بخصوص سیم کارت که کلید مشترک (Ki) را در خود دارد ، مقدار کلید و RAND که در عملیات اعتبار سنجی استفاده می شدند را به الگوریتم A8 اعمال میکند . نتیجه یک کلید رمز ی Kc ۶۴ بیتی است که به عنوان ورودی به الگوریتم A5 موبایل داده می شود و یک رشته کلید ایجاد می کند که برای رمز گذاری سیگنالهای صدا در حالت ارسال و رمز گشایی سیگنال

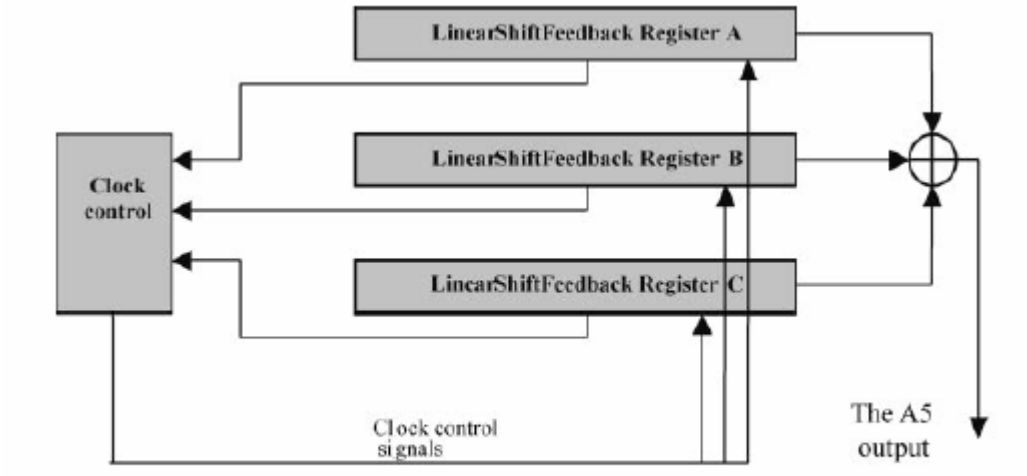

Figure 5.8 The A5 keystream generation

صدای دریافت شده در حالت دریافت استفاده می شود . در طول این زمان ، BTS بعد از SRES اعتبار سنجی به حالت رمزی سوئیچ می کند و مشابها کلید Kc را بکار می برد تا سیگنالهای صدای روی همان کانال را رمز گذاری کند . بنا براین تماس که از طریق واسط Um بین MS و BST منتقل می شود رمز گذاری شده در نتیجه محرمانه است .

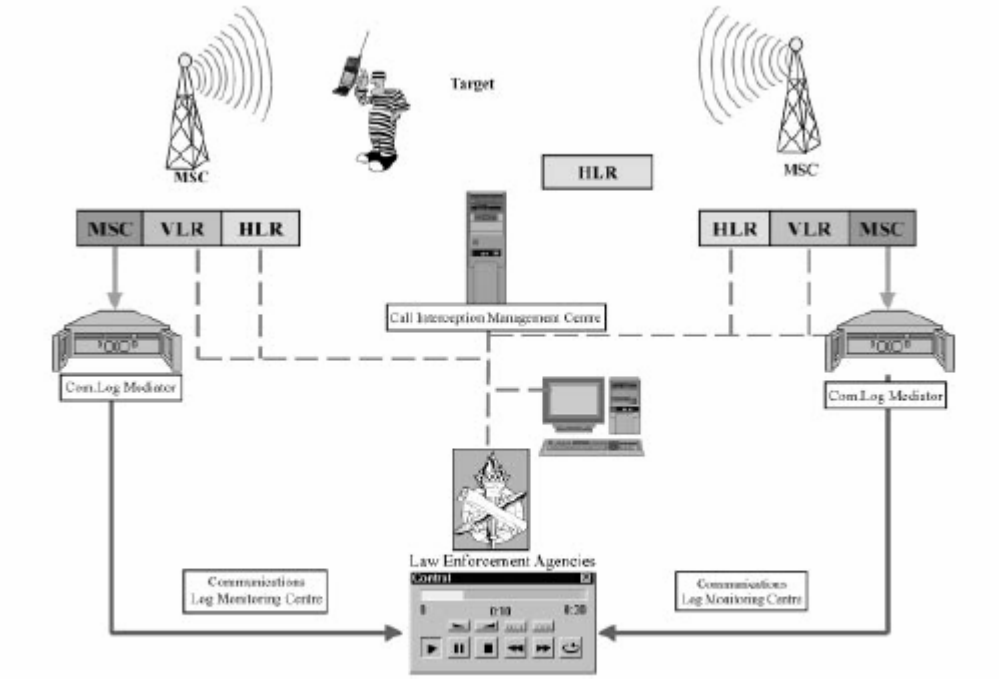

Figure 5.9 A GSM monitoring centre

الگوریتم A3 برای اعتبار سنجی کاربر ، A5 برای رمز گذاری پیغام و A8 الگوریتم تولید کننده کلید برای پشتیبانی A5 است که تقریبا مقایسه ضعیفی با دیگر استانداردهاست . هر دو الگوریتم های A8, A3 به همراه کلید واحد مشترک (Ki) در سیم کارت اجرا می شوند و بنا بر این قابل انتقال به یک روش امن است در زمانیکه کاربر از طریق اپراتور شبکه های دیگر مسیر یابی می کند .ا لگوریتم A5 یک جزء ثابت در سخت افزار موبایل GSM است که برای رمز گذاری سه خط رجیستر فیدبک را استفاده می کند تا یک کلید مؤثر با طول ۶۴ بیت را بدهد . Kc که طولش ۶۴ بیت است درون رجیسترهایی که در مدت زمان خاصی کلاک اشان می خورد ، قرار می گیرد و خروجی ۲۲۸ بیتی دارد که اتصال بالا اش ۱۱۴ بیت و اتصال پائینش ۱۱۴ بیت رمز گذاری شده می باشد .

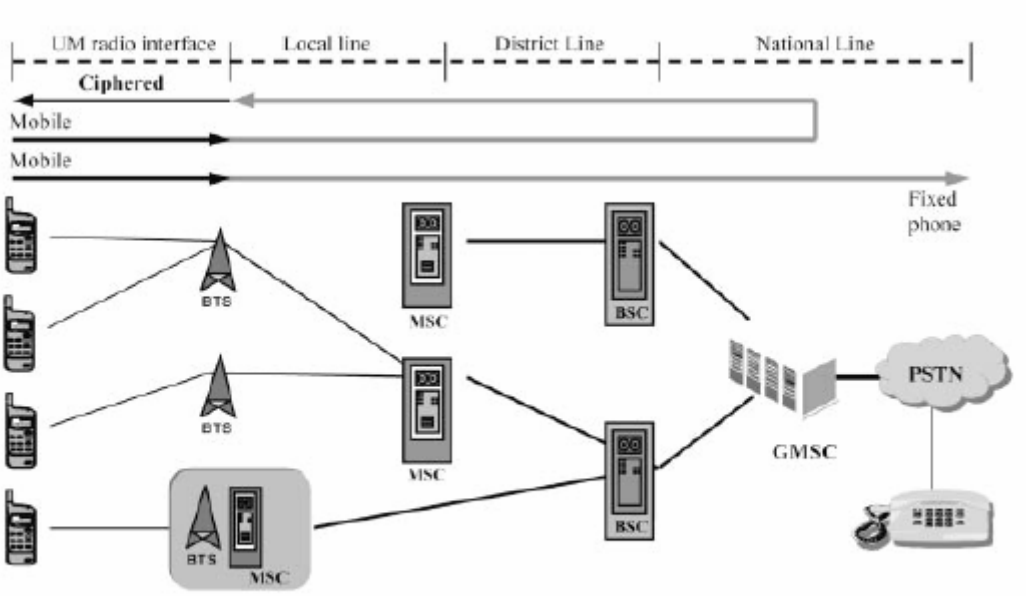

Figure 5.10 The extent of standard GSM encryption

تعداد زیادی ادعا و شایعه در مورد نقصهای موجود در الگوریتم GSM توسط افراد مختلف وجود دارد ولی هیچکدام قابل اثبات با دلیل و مدرک نبودند . هر چند که تعداد زیاد حمله ها امنیت GSM را تحت تأ ثیر قرار داده و افراد را به ظن می برد که آن ادعا ها درست هستند . به بیان دقیقتر بیشتر تولید کنندگان قطعات رمز گذاری ، فرض کرده اند که در این الگوریتمها تناقض وجود دارد . این فرض با نام " فرضیه کرچوف" هم شناخته شده و تمام الگوریتمها و تجهیزات امنیتی بر همین اساس ساخته شده اند . در عوض امنیت مبتنی بر اطمینان زیادی است که کلید رمز و تغییرات مداوم آن ایجاد می کند . متاسفانه در حال حاظر Ki در GSM یک کلید ماندگار است و در نتیجه آسیب پذیر می باشد . برای اجتناب از این خطر تغییرات بیشتر Ki برای امنیت سیستم مورد نیاز است ولی در عین حال ممکن است برای کسانیکه به Ki دسترسی دارند مشکل ساز باشد .

یک نکته دیگر این است که تمام الگوریتمهای GSM در انگلستان وبرای ETSI و گروه سازندگان اصلی GSM ایجاد شده . در نتیجه یک محدودیت دردسر ساز برای گسترش این سیستم می باشد.

برای گسترش GSM به ناحیه دیگر سه مرحله امنیتی کانالها لازم است . از جمله الگوریتم رمز گذاری A5 ، A5/1، A5/2 و رمز گشایی . ورژن با بیشترین امنیت A5/1 است که در کشورهایی که عضو (CEPT) هستند مورد استفاده قرار می گیرند . دومین سطح A5/2 برای گسترش به کشورهایی

خارج از این دسته (مانند کشورهای مرکزی و غربی اروپا) استفاده می شود . در سطح آخر و برای کشورهایی مثل روسیه ، اصلا رمز گذاری وجود ندارد .

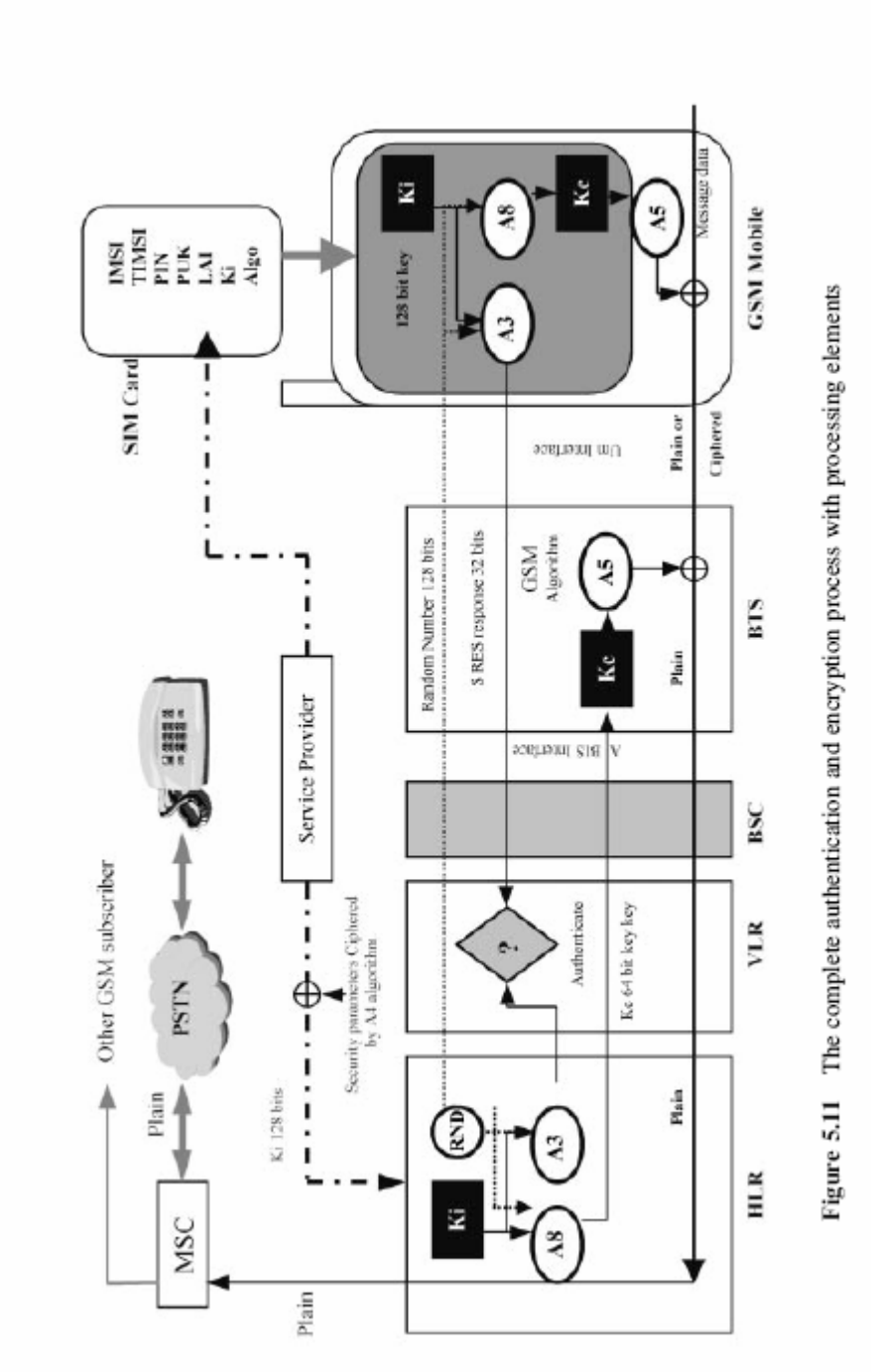

Figure 5.11 The complete authentication and encryption process with processing elements