پردیس بین المللی دانشگاه تبریز

گروه علوم کامپیوتر

پایاننامه

برای دریافت درجه کارشناسی ارشد در رشته علوم کامپیوتر

عنوان

یک راهکار برای افزایش امنیت پیام‌کوتاه

استاد راهنما

دکتر آیاز عیسی زاده

استاد مشاور

دکتر جابر کریم پور

پژوهشگر

ناصر فرشباف صبوری

بهمن ماه ۹۳

نام خانوادگی دانشجو: فرشباف صبوری **نام**: ناصر

عنوان پایان نامه/رساله: یک راهکار برای افزایش امنیت پیام‌کوتاه

استاد راهنما: دکتر آیاز عیسی زاده
استاد مشاور: دکتر جابر کریم پور

مقطع تحصیلی: کارشناسی ارشد **رشته**: علوم کامپیوتر **دانشگاه**:پردیس بین المللی دانشگاه تبریز

تاریخ فارغ التحصیلی: **تعداد صفحه**: ۹۰

کلید واژه ها: موبایل بانک، SMS ،پیام‌کوتاه، پروتکل، امنیت

چکیده

امروزه پیام کوتاه به یک ابزار محبوب در ارتباطات افراد و گسترش کسب و کارها تبدیل شده است. در سال ۲۰۱۳ بیش از ۶/۱ تریلیون پیام کوتاه ارسال شده است. در زندگی روزمره برخی اوقات افراد اقدام به تبادل اطلاعات محرمانه نظیر کلمات عبور و سایر اطلاعات حساس دیگر از طریق پیام کوتاه می نمایند. اما آیا این ارتباط امن است؟ زمانیکه اطلاعات حساس با استفاده از پیام کوتاه مبادله می شود، بسیار مهم است که این اطلاعات از انواع استراق سمع‌ها محافظت شده و نیز تضمین شود که منشأ فرستنده پیام معتبر است.

سرویس پیام کوتاه یا SMS، سرویسی است که امکان ارسال پیام متنی در یک شبکه تلفن همراه را میسر می‌سازد. در مقالات علمی امنیت در کنار واژه‌هایی مانند محرمانگی، یکپارچگی، صحت، غیر قابل انکار بودن، حفاظت از حریم خصوصی و حفاظت از حریم داده‌ها ذکر شده است. پیام کوتاه، فاقد هر گونه ویژگی امنیتی می‌باشد و ارتباطات بین دو ایستگاه بدون هرگونه تأیید هویت اولیه برقرار می‌شود و متن پیامک نیز بدون امضای دیجیتالی و یا رمزنگاری مبادله می‌گردد. در نتیجه بسیاری از سرویس‌هایی که با تکیه بر پیام کوتاه عرضه می‌شوند، با مشکل ضعف امنیتی مواجه می‌باشند. این مشکل توسط جامعه علمی شناسایی و مکرراً بیان شده است.

این پژوهش درصدد ارایه یک راه‌کار برای افزایش امنیت پیام کوتاه می‌باشد که در آن، روشی طراحی خواهد شد که دو ایستگاه را قادر می‌سازد پیام‌های کوتاه را به صورت رمزنگاری شده و یا با امضای دیجیتالی مبادله نمایند. اساس این روش استفاده از ویژگی‌های امنیتی در سطح برنامه است که از طریق اجرای یک نرم افزار خاص بر روی ایستگاه‌های ارتباطی به منظور امن سازی تبادل پیام کوتاه تحقق می‌یابد.

کلمات کلیدی: موبایل بانک، SMS ،پیام‌کوتاه، پروتکل، امنیت

فهرست مطالب

عنوان شماره صفحه

فهرست جداول

عنوان **شماره صفحه**

فهرست شکل ها

عنوان **شماره صفحه**

فصل ۱

مقدمه

۱– ۱ مقدمه:

تجارت و کسب وکار، یکی از مهمترین حوزه‌هایی است که با بکارگیری فناوری‌های نوین اطلاعاتی و ارتباطی و اینترنت به سرعت و بشدت تحت تاثیر قرار گرفت. ضریب نفوذ ابزارهای موبایلی بالاتر از هرفناوری دیگری است و این مساله، تجارت موبایلی را به شکل انقلاب جهانی درآورده است که با همان وقوع در کشورهای پیشرفته، درکشورهای درحال توسعه نیز درحال رخ دادن است. یکی از خدمات ارائه شده توسط موبایل،نرم افزارهای مبتنی بر پیام کوتاه از جمله بانکداری همراه می‌باشد. بانکداری همراه در قسمت های مختلف جهان با موفقیت بسیار زیادی همراه بوده است. دلیل اصلی که موسسات مالی علاقمند به ارائه خدمات بانکداری هستند این است که این روش کانال ارتباطی جدید و قدرتمندی را با استفاده از تلفن همراه در اختیار آنها قرار می دهد. بانکداری تلفن همراه یک حوزه جدید پژوهشی است. در حال حاضر بانک ها به شدت به دنبال گسترش ارائه خدمات خود به مشتریان از طریق تلفن‌همراه هستند، این رشد از زمانی شروع شد که از یک سو سیستم‌های مخابراتی بی‌سیم دچار جهشی در پیشرفت فن آوری شدند و از سوی دیگر عدم محدودیت مکانی، ضریب نفوذ بالا، شخصی‌سازی و همراه همیشگی افراد بودن باعث شد محبوبیت در این زمینه بیشتر از سایر خدمات بانکداری گردد. مشکلات بانکداری مبتنی بر پیام‌کوتاه از آنجا ناشی می شود که ارسال پیام کوتاه در شبکه موبایل به طورکامل امن نیست، و این موضوع به معایب موجود درمعماری GSM برمی‌گردد که منجر به کاهش امنیت در ارسال پیام کوتاه می شود.

۱-۲ اصطلاحات

GSM[۱]: یکی از رایجترین سیستم‌های مخابراتی بدون سیم در جهان می‌باشد که اپراتورهای موجود در ایران نیز از این سیستم ها استـفاده می‌نمایند.

بانکداری همراه: به شیوه‌ای اطلاق می‌گردد که در آن از سرویس‌های ارئه شده برروی تلفن همراه مشتریان جهت انجام تراکنش های بانکی و مالی و خرید و فروش استفاده می شود.

ارتباط PUSH**:** در ارتباط PUSH بانک در ازای هر تراکنش که روی حساب مشتری روی می‌دهد از طریق پیامک به او پاسخ می‌دهد[۱۱].

ارتباطPULL**:** در ارتباط PULL بانک بنا به درخواست مشتری پاسخ خاصی را برای او ارسال می‌دارد مانند تقاضای موجودی حساب.

Spoofing: به‌عملی اطلاق می‌گردد که در آن فرستنده جعلی خودرا به عنوان فرستنده اصلی جا می‌زند.[۱۲]

GPRS[۲]: نسل سوم تلفن همراه می‌باشند که در آنها سرویس‌های رادیویی و اینترنت پیشرفت کرده‌اند.[۱۲]

عدد IMSI[۳]**:** عددی منحصر بفرد در کل جهان که در سیم‌کارت هر مشترک تعبیه شده که شبکه اپراتور همراه برای شناسایی مشترک جهت استفاده از خدمات سـیستم‌کارت از این عدد اسـتفاده می‌کند، این عدد از یک سـیم‌کارت به سـیم‌کارت دیگر متفـاوت می‌باشد[۱۱].

[۱] Global System for Mobile Communications
[۲] General Packet Radio Service
[۳] International Mobile Subscriber Identity

الگوریتم های A5 **و** A8 : الگوریتم‌های رمزنگاری هستند که بصورت سخت‌افزاری در انواع گوشی‌ها طراحی شده‌اند و برای امنیت اطلاعات و حفظ اصل محرمانگی اطلاعات انتقالی از آنها استفاده می‌شود.[۱۲].

PIN و PUK: سیم کارت مشترک توسط این شناسه محافظت می‌شود، چنانکه کاربر چند بار PIN را اشتباه وارد کند سیم کارت قفل می شودو از او PUK تقاضا می‌شودکه در صورت اشتباه وارد کردن آن برای چند بار متوالی، سیم‌کارت دسترسی به اطلاعات محلی و توابع احراز اصالت خود را بطور دائم غیر فعال می‌کند[۱۱].

رمزنگاری:

رمزنگاری استفاده از تکنیکهای ریاضی برای ایجاد امنیت در اطلاعات است، به عبارتی رمزنگاری دانشی است جهت تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم مشخص می‌باشد، بطوریکه فقط شخص رمز کننده یا کسی که کلید آن را در اختیار داشته باشد قادر به رمزگشایی از آن باشد، رمزنگاری بسته به نوع آن ممکن است با یک کلید یا دو کلید انجام گیرد.

هنگامی که با امنیت اطلاعات سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت اصول اصلی ایجاد امنیت اطلاعات می‌باشندکه از طریق رمزنگاری تامین می‌شود اغلب این مساله باید تضمین شود که یک پیغام فقط می‌تواند توسط کسانی خوانده شود که پیغام برای آنها ارسال شده‌است و دیگران این اجازه را ندارند. روشی که تامین کننده این مساله باشد "رمزنگاری" نام دارد. رمزنگاری هنر تغییر اطلاعات است بطوریکه هیچکس به غیر از دریافت کننده موردنظر نتواند محتوای پیغام را بخواند.

رمزنگاری اصطلاحات مخصوص به خود را دارد. برای درک عمیق‌تر به مقداری از دانش ریاضیات نیاز است. برای محافظت از اطلاعات اصلی[۴]، آنرا با استفاده از یک کلید (رشته‌ای محدود از بیتها) بصورت رمز در می‌آوریم تا کسی که دیتای حاصله را می‌خواند قادر به درک آن نباشد. اطلاعات رمزشده [۵]بصورت یک سری بی‌معنی از بیتها بدون داشتن رابطه مشخصی با دیتای اصلی بنظر می‌رسد. برای حصول متن اولیه دریافت‌کننده آنرا رمزگشایی می‌کند.

رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید. الگوریتم یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها بعنوان استانداردها یا مقالات ریاضی منتشر شده‌اند. کلید، یک رشته از ارقام دودویی (صفر و یک) است که بخودی‌خود بی‌معنی است. رمزنگاری مدرن فرض می‌کند که الگوریتم شناخته شده است یا می‌تواند کشف شود، کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پیاده‌سازی تغییر می‌کند. رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند.

MAC: یک چک تایید پیام یا MAC [۶]یک الگوریتم ثابت با تولید یک امضاء برروی پیام با استفاده از یک کلید متقارن است. هدف آن نشان دادن این مطلب است که پیام بین ارسال و دریافت تغییر نکرده است. هنگامی که رمزنگاری توسط کلید عمومی برای تایید هویت فرستنده پیام استفاده می‌شود، منجر به ایجاد امضای دیجیتال[۷] می‌شود.

Public Key : کلید عمومی اعداد یا کلماتی که با یک شخص یا سازمان در ارتباط می‌باشد. کلید عمومی جزئی از جفت کلید عمومی/خصوصی می‌باشد وبه صورت عمومی در دسترس کسانی که قصد انتقال اطلاعات رمز شده را دارند، می‌باشد[۲].

---

[۴] Plaintext
[۵] Ciphertext
[۶] Message Authentication Check
[۷] Digital Signature

Private Key: کلید خصوصی اعداد یا کلماتی که با یک شخص یا سازمان در ارتباط می‌باشد. کلید خصوصی جزئی از جفت کلید عمومی/خصوصی می‌باشد. کلید خصوصی فقط در دسترس مالک جفت کلید عمومی/ خصوصی می‌باشد و برای بازگشایی اطلاعاتی که توسط کلید عمومی رمزگذاری شده استفاده می‌شود. ایجادکننده های جفت کلید برای ایجاد یک جفت کلید عمومی و خصوصی طبق یک الگوریتم رمزگذاری مشخص استفاده می‌شود[۲].

Key Factories: برای تبدیل کلید های نامشخص به کلیدهای مشخص به کار می‌رود.[۱]

Keystores: بانکی که برای مدیریت تعدادی از کلید ها به کار می‌رود.[۱]

الگوریتم های رمزگذاری : الگوریتم‌ها و روشهایی که برای رمزگذاری اطلاعات به کار می‌رود. RSA و DES نام دو تا از معروفترین الگوریتم ها می‌باشد.

طراحی الگوریتمهای رمزنگاری مقوله‌ای برای متخصصان ریاضی است. طراحان سیستمهایی که در آنها از رمزنگاری استفاده می‌شود، باید از نقاط قوت و ضعف الگوریتمهای موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصمیم‌گیری داشته باشند. اگرچه رمزنگاری از اواخر دهه ۴۰ و اوایل دهه ۵۰ بشدت پیشرفت کرده است، اما کشف رمز نیز پابه‌پای رمزنگاری به پیش آمده است و الگوریتمهای کمی هنوز با گذشت زمان ارزش خود را حفظ کرده‌اند.

رمزنگاری متقارن:

روش متقارن[۸] روشی است که در آن هر دو طرفی که قصد رد و بدل اطلاعات را دارند از یک کلید مشترک برای رمزگذاری و نیز بازگشایی رمز استفاده می‌کنند. در این حالت بازگشایی و رمزگذاری اطلاعات دو فرآیند معکوس یکدیگر می‌باشند. مشکل اصلی این روش این است که کلید

[۸] Symmetric

مربوط به رمزگذاری باید بین دو طرف به اشتراک گذاشته شود و این سوال پیش می‌آید که دو طرف چگونه می‌توانند این کلید را به طور امن بین یکدیگر رد و بدل کنند؟ در پاسخ باید گفت که کانال امنی باید وجود داشته باشد و یا از رمزنگاری نامتقارن برای تبادل امن کلیدها استفاده کرد. انتقال از طریق انترانت و یا به صورت فیزیکی تا حدی امن می‌باشد اما در انتقال آن در اینترنت به هیچ وجه درست نمی‌باشد.در این قبیل سیستم ها، کلید های رمزنگاری و رمزگشایی یکسان هستند و یا رابطه‌ای بسیار ساده با هم دارند .این سیستم ها را سیستم‌های متقارن یا " تک کلیدی " می‌نامیم. به دلیل ویژگی ذاتی تقارن کلید رمزنگاری و رمزگشایی، مراقبت و جلوگیری از افشای این سیستم‌ها یا تلاش در جهت امن ساختن آنها لازم است در بر گیرنده " جلوگیری از استراق سمع " و " ممانعت از دستکاری اطلاعات " باشد [۲].

رمزنگاری نامتقارن:

رمزنگاری نامتقارن[۹] روشی است که برای حل مشکل انتقال کلید در روش متقارن ایجاد شد. در این روش به جای یک کلید مشترک از یک جفت کلید به نام های کلید عمومی و خصوصی استفاده می‌شود. در این روش از کلید عمومی برای رمزگذاری اطلاعات استفاده می‌شود. طرفی که قصد انتقال اطلاعات را به صورت رمزگذاری شده دارد اطلاعات را رمزگذاری کرده و برای طرفی که مالک این جفت کلید است استفاده می‌شود. مالک کلید، کلید خصوصی را پیش خود به صورت محرمانه حفظ می‌کند. در این دسته، کلیدهای رمزنگاری و رمزگشایی متمایزند و یا اینکه چنان رابطه پیچیده‌ای بین آنها حکم فرماست که کشف کلید رمزگشایی با در اختیار داشتن کلید رمزنگاری، عملا ناممکن است.[۲]

درمقایسه الگوریتم‌های رمزنگاری متقارن و الگوریتم‌های کلید عمومی بحث‌های زیادی شده که کدام یک از این الگوریتم‌ها بهترند اما جواب مشخصی ندارد. البته بررسی هایی روی این سوال

[۹] Asymmetric

شده به طور مثال Needham و Schroeder بعد از تحقیق به این نتیجه رسیدند که طول پیغامی که با الگوریتم های متقارن میتواند رمزنگاری شود از الگوریتم های کلید عمومی کمتر است. و با تحقیق به این نتیجه رسیدند که الگوریتم های متقارن الگوریتم‌های بهینه‌تری هستند. اما وقتی که بحث امنیت پیش می آید الگوریتم های کلید عمومی کارایی بیشتری‌دارند. و بطور خلاصه می‌توان گفت که الگوریتم‌های متقارن دارای سرعت بالاتر و الگوریتم های کلید عمومی دارای امنیت بهتری هستند[۲]. در ضمن گاهی از سیستم ترکیبی از هردو الگوریتم استفاده میکنند که به این الگوریتم ها الگوریتم های ترکیبی[۱۰] گفته می‌شود. اما اگر به طور دقیق تر به این دو نگاه کنیم آنگاه متوجه خواهیم شد که الگوریتم‌های کلید عمومی و الگوریتم‌های کلید متقارن دارای دو ماهیت کاملا متفاوت هستند و کاربرد های متفاوتی دارند به طور مثال در رمزنگاری‌های ساده که حجم داده‌ها بسیار زیاد است از الگوریتم متقارن استفاده می‌شود زیرا داده‌ها با سرعت بالاتری رمزنگاری و رمزگشایی شوند.

Key Agreement : همانطور که در بالا گفته شد روش نامتقارن یک مشکل اساسی دارد و آن اینست که هر شخص نیاز به کلید عمومی و خصوصی مربوط به خود را دارد و باید برای انتقال اطلاعات آنرا برای طرف مقابل بفرستد. یک راه برای حل مشکل استفاده از کلید عمومی، مکانیزمی به نام Agreement Key می‌باشد که بر طبق آن یک توافق بر روی کلید مخفی بین طرفین به وجود می‌آید و به این ترتیب نیازی به انتقال کلید نمی‌باشد. وقتی که یک بار بر روی یک کلید مشترک توافق حاصل شد از آن می‌توان برای رمزگذاری و رمزگشایی اطلاعات مربوطه استفاده کرد. مراحل انتقال اطلاعات در این روش به صورت زیر می‌باشد:

فرستنده ابتدا یک جفت کلید عمومی و خصوصی ایجاد کرده و کلید عمومی را همراه با مشخصات الگوریتم به سمت طرف مقابل می‌فرستد. طرف مقابل نیز یک جفت کلید عمومی و

[۱۰] Hybrid

خصوصی همراه با مشخصات الگوریتم فرستنده ساخته و کلید عمومی را برای فرستنده می‌فرستد. - فرستنده یک کلید مخفی بر اساس کلید خصوصی خود و کلید عمـــومی طرف مقابل ایجاد میکند. طرف مقابل نیز با استفاده از کلید خصوصی خود و کلید عمومی فرستنده یک کلید مخفی می‌سازد. این‌کار با پروتکل‌هایی از جمله پروتکل دیفی هلمن [۱۱]انجام می گیرد.

پروتکل تبادل کلید دیفی هلمن، یک پروتکل رمزنگاری است که با استفاده از آن، دو نفر یا دو سازمان، می‌توانند بدون نیاز به هر گونه آشنایی قبلی، یک کلید رمز مشترک ایجاد و آن را از طریق یک مسیر ارتباطی غیر امن، بین خود تبادل نمایند. این پروتکل، اولین روش عملی مطرح شده برای تبادل کلید رمز در مسیرهای ارتباطی غیر امن است و مشکل تبادل کلید رمز در رمزنگاری کلید متقارن را آسان می‌سازد.

[۱۱] Diffii Hellman

۱-۳ بیان مساله

مساله مورد بحث دراین رساله بررسی و تحلیلی است واقع بینانه، مروری انتقادی از کارهای انجام گرفته درخصوص امنیت SMS می‌باشد. سرویس پیام‌کوتاه یا SMS مکانیزمی جهت انتقال پیام‌کوتاه را در وسایل بی‌سیم دراختیار می‌گذارد. این سرویس از یک مرکز سرویس پیام‌کوتاه (SMSC[۱۲]) بهره می گیرد که به عنوان ذخیره و ارسال برای پیام های کوتاه عمل می‌کندو شبکه بی‌سیم، مسئولیت انتقال پیام‌های کوتاه بین SMSC و ادوات سیار را برعهده می‌گیرد. پیام از طریق یک مسیر سیگنال مجزا ارسال می‌شود و قابلیت انتقال همزمان با صوت، داده و دورنگار را دارد. در مقایسه با برخی سرویس های متنی موجود، این سرویس چنان طراحی شده که ضمانتی برای دریافت پیام های متنی در مقصد را نیز فراهم آورد. بدین ترتیب که فرستنده پیام‌کوتاه پس از ارسال، پیامی مبتنی بر ارسال موفقیت‌آمیز پیام‌کوتاه از شبکه دریافت می‌داردو پیام کوتاه ذخیره شده در SMSC تا زمان انقضای مدت اعتبارآن و تا زمانی که مشترک هدف در دسترس نباشد باقی می‌ماند و بمحض در دسترس قرار گرفتن مشترک هدف، پیام کوتاه ذخیره شده برای وی ارسال خواهد شد.یکی دیگر از ویژگی‌های SMS ارسال بصورت پاکتی و کم بودن پهنای باند انتقال آن است. سرویس پیام کوتاه امکان تبادل پیامهای کوتاه ۱۴۰ بایتی (حداکثر ۱۶۰ کاراکتری) را ممکن می‌سازد. بطورکلی مشکلات امنیتی که SMS بعنوان یک روش انتقال داده از شبکه سیار مورد استفاده به ارث می برد، تعدادی آسیب پذیری اضافه که معمولا ارتباطی به شبکه سیار مورد استفاده ندارد. درخصوص دسته اول، درواقع کلیه مشکلات امنیتی GSM به تمام سرویس‌ها و مسیرهای انتقال داده در GSM و از جمله SMS قابل اعمال می باشد. چراکه حملات ذکر شده کلیه داده‌ها و سیگنالینگ مبادله شده را هدف قرار میدهد[۶]. کارها تکنیکها، الگوریتم‌ها در این پایاننامه بر اساس ضوابط زیر مورد بررسی قرار خواهند گرفت:

[۱۲] Small Message Service Centre

۱)ضابطه اول ما که کارهای مربوطه باید بر اساس آن مورد بررسی قرار گیرند عبارتست از تمامیت و درستی[۱۳] است. بعبارتی پیام پس از ایجاد و انتقال از گوشی فرستنده باید بدون کوچکترین تغییری به گیرنده برسدو یا درصورت وقوع هرگونه تغییری گیرنده ازآن متوجه شود.

۲) ضابطه دوم ما که کارهای مربوطه باید بر اساس آن مورد بررسی قرار گیرند عبارتست از سندیت و تصدیق[۱۴] است.کاربـر درهنگام شـروع عملیات بانکی بوسیله موبایل PIN خود را وارد می‌کند که در بخش سرور بانک از این PIN جهت شناسایی کاربر استفاده می‌شود[۱۱].

۳) ضابطه سوم ما که کارهای مربوطه باید بر اساس آن مورد بررسی قرار گیرند عبارتست از قابلیت اعتماد[۱۵] است، که این مورد هم در هنگام انتقال وجه بوسیله رمز کردن پیام با یک رمزعبور یکبارمصرف، مفهوم پیدا می‌کند، فرض می شود که تنها مشتری و بانک از این رمز عبور آگاهی دارند.

۴) ضابطه چهارم ما که کارهای مربوطه باید بر اساس آن مورد بررسی قرار گیرند عبارتست ازعدم انکار[۱۶] است. بطوریکه کاربر نتواند پس از انجام عملیات بانکی منکر ارسال پیام از طرف او باشد.

بنابراین باید راهکاری ارائه گردد که یک انتقال امنی برای پیامک در طول مسیر بین فرستنده و گیرنده هدف که اینجا سرور بانک است ایجاد کند که در آن اصول امنیتی تمامیت و درستی داده‌ها، سندیت و تصدیق، قابلیت اعتماد و عدم انکار، حفظ شود.

[۱۳] Integrity
[۱۴] Authentication
[۱۵] Confidentiality
[۱۶] Non Repudiation

۱–۴ اهداف پایاننامه

هدف این پایاننامه بررسی امنیت GSM و درنتیجه امنیت ارسال پیامک از طریق این سیستم می‌باشد، که در کل امنیت موبایل بانک‌ها و سایر نرم‌افزارهای متکی بر پیام‌کوتاه به میزان امنیت این دو بستگی دارد. بنابراین سعی خواهیم کرد تا ضعف‌های موجود و نوع حملات ممکن به سیستم را بررسی نمائیم. الگوریتم‌های رمزنگاری موجود در GSM را بررسی، مقایسه و در نهایت راه کاری جهت افزایش امنیت این نرم‌افزارها که کانال ارتباطی آنها پیام‌کوتاه است ارائه نمائیم.

۱–۵ نظریه

بر اساس اهداف فوق، این نظریه مطرح می‌شود که می‌توان راه‌کاری ارائه داد که امنیت پیام کوتاه را در تمام طول مسیر درGSM تامین نماید؛ این امر باعث بالا رفتن امنیت بانکداری همراه بر اساس پیام کوتاه خواهد شد.

در این پژوهش ما سعی خواهیم کرد ابتدا نقاط ضعف، مشکلات و راههای نفوذ در GSM را شناسایی و مورد بررسی قرار دهیم ، سپس طرحی را در قالب یک پروتکل امنیتی پیشنهاد دهیم که بتواند امنیت پیام کوتاه را بصورت انتها به انتها در طول شبکه GSM تامین نماید، همچنین با استفاده از زبان برنامه نویسی دلفی این طرح را پیاده سازی خواهیم کرد.

درواقع هدف ارسال اطلاعات بصورت رمزشده در طول شبکه است که در یک انتها (فرستنده یا گیرنده) اطلاعات رمز شده و در انتهای دیگر رمزگشایی انجام می گیرد تا اطلاعات در طول مسیر شبکه بصورت شکل اصلی آن ارسال نگردد ، از این جهت است که به این طرح روش انتها به انتها گویند.

پروتکل طراحی شده باید تمام اصول مربوط به سرویس‌های امنیتی که شامل قابلیت اعتماد، تمامیت داده، سندیت و عدم انکار مطابقت داشته باشدو از سرعت و هزینه قابل قبولی برخوردار باشد

شکل ۱-۱ : نمای کلی از طرح در تامین امنیت انتها به انتها

با ارائه این طرح سعی داریم امنیت سیستم های مبتنی بر پیام کوتاه که از آن بعنوان یک کانال ارتباطی استفاده می نمایند را افزایش دهیم از این سیستم ها می توان به موبایل بانکها،نرم افزارهای معاملات آن لاین در بورس ، انواع نرم افزارهای پرداخت و... نام برد

در اینجا ساختار نرم افزارهای مبتنی بر پیام کوتاه و سیستم بانکداری امن به سه رده، تقسیم می‌شود. فرستادن آن در قالب یک پیام از طریق شبکه GSM به سرور مقصد، بخش سرور بانک که بطور مرتب پیام های ورودی را دریافت کرده و آنها را به شکل برنامه‌ای قابل تفسیر تبدیل می‌کند و بخش پایگاه داده که شامل تمامی اطلاعات بانکی و امنیتی کاربران است، هدف ما امن سازی پیام کوتاه در این سیستمها است که بدین طریق کانال ارتباطی این سیستمها را امن خواهیم کرد.

در راستای این هدف تلاش خواهیم کرد از مناسبترین تکنیک های رمزنگاری و رمزگشایی برای این طرح استفاده نمائیم.

در طول نگارش این پایاننامه سعی کردیم طرح را با بررسی مثالی پیش ببریم، این مثال را سیستم موبایل بانک که کانال ارتباطی آن با سرور خدمات دهنده پیام کوتاه می باشد، انتخاب کرده ایم.