دانشکده فنی ومهندسی

پایان نامه کارشناسی ارشد

رشته مهندسی پزشکی گرایش بیو الکتریک

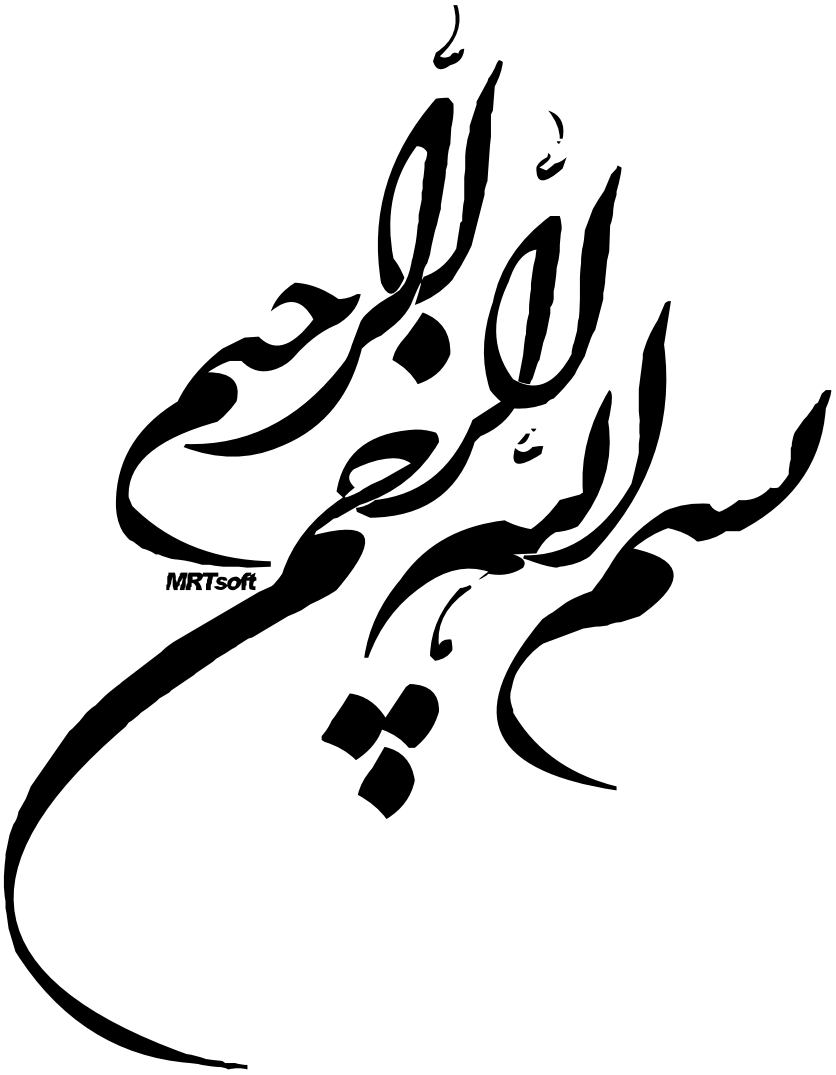
عنوان پایان نامه :

امکان سنجی حمله به کارت هوشمند سلامت از طریق RFID

استاد راهنما: جناب آقای دکترمحمد علی دوستاری

نگارش :روح الله حشمتی

زمستان۸۸


بسم الله الرحمن الرحیم
MRTsoft

دانشگاه شاهد

دانشکده فنی و مهندسی

صورت جلسه هیئت داوران رساله کارشناسی ارشد

جلسه دفاعیه پروژه کارشناسی ارشد مربوط به آقای **روح الله حشمی** به شماره دانشجویی**۸۴۷۵۲۰۰۰۲**در رشته **مهندسی پزشکی** با عنوان "**امکان سنجی حمله به کارت هوشمند سلامت از طریق RFID**" به ارزش **۶ واحد** در روز**۸۸/۱۲/۲۴** در دانشکده فنی و مهندسی با حضور افراد ذیل تشکیل شد، نتیجه به قرار زیر است :

☐ پروژه نامبرده با نمره قابل قبول می‌باشد.

☐ پروژه نامبرده مردود می‌باشد.

☐ پروژه نامبرده به شرط انجام اصلاحات جزیی قابل قبول می‌باشد. نمرهٔ دانشجو متعاقباً اعلام می‌شود.

☑ نام استاد راهنمای اول ارد. درستاری	دانشگاه : شاهد	امضاء
☐ نام استاد راهنمای دوم	دانشگاه :	امضاء
☐ نام استاد مشاور اول	دانشگاه :	امضاء
☐ نام استاد مشاور دوم	دانشگاه :	امضاء
☐ نام داور اول ارد. حدائق	دانشگاه : صنعتی شیراز	امضاء
☐ نام داور دوم ارد. بیدار	دانشگاه : شاهد	امضاء
☐ نام داور سوم	دانشگاه :	امضاء
☐ نام داور چهارم	دانشگاه :	امضاء
☐ نام نماینده معاونت پژوهشی دکتر خیاط		امضاء

۸۸/۱۲/۲۴

تقدیم به:

این تلاش ناچیز را با تمام وجود به همسر و فرزند عزیزم تقدیم می دارم امید است که سایه پر مهرشان همواره نوازشگر روح خسته ام بوده و دعای خیرشان همواره و در همه ایام حافظ و پشتیبان اینجانب در گذر از راه های پر پیچ و خم زندگی باشد.

تشکروقدرانی:

در ابتدا وظیفه خود میدانم که از راهنمایی ها وکمک های بی شائبه و صمیمانه استاد محترم جنا ب آقای دکترمحمـد علـی دوستاری که در طی انجام پروژه و تدوین پایان نامه نهایت مساعدت را در حق اینجانب مبذول داشتند کمال تقـدیر و تشـکر بنمایم.

چکیده :

امروزه کارتهای هوشمند در تعاملات اقتصادی و اجتماعی نقش بسزایی دارند (کارتهای هوشمند سوخت، کارتهای اعتباری، کارتهای هوشمند درقالب SIM card، کارتهای هوشمند سلامت. visa کارت، کارتهای حضور وغیاب و...). گاهی کارتهای هوشمند حاوی کلید خصوصی و سری افراد نیز هستند و لیکن به نحوی طراحی شده اند که کلید خصوصی یا هرگز از کارت خارج نشود و به هیچ وجه در اختیار هیچ کس حتی صاحب آن کارت قرارنگیرد و یا انتقال داده های سری تحت شرایط خاص و مکانیزمهای احراز هویت انجام شود. کارتهای هوشمند مکرراً از رمزنگاری جهت اعتبار سنجی مصرف کننده و ذخیره کردن اطلاعات محرمانه استفاده می کند. کارتهای هوشمند از جمله سیستم هایی است که در آن از مدرن ترین سیستمهای ایمنی استفاده می شوند. لذا حمله به کارتهای هوشمند و به دست آوردن کلیدهای خصوصی یکی از مسائلی است که نظر هکرها را به خود جلب کرده است. از اینرو امنیت داده کارتهای هوشمند یکی از مهمترین مواردی است که محققان و دانشمندان در این زمینه کار می کنند و نقاط ضعف و قوت آنها را مورد بررسی قرار می دهند. در این پایان نامه حمله آنالیز توان به کارتهای هوشمند از جمله RFID مورد بررسی قرارگرفته است و نتایج به دست آمده حاکی از این است که روش حمله آنالیز توان روشی قوی جهت حمله به کارتهای هوشمند و وسایل رمز نگاری می باشند حتی اگر این وسایل به انواع ضدحمله های آنالیز توان مجهز باشند. حمله آنالیز توان با استفاده از نمونه برداری از توان مصرفی وسیله رمز نگاری و مقایسه با توان مدل شده می تواند کلید الگوریتم رمزنگاری را استخراج نماید.

فصل۱: پیشگفتار

فصل۲ : معرفی الگوریتم رمزنگاری و احراز هویت در کارت هوشمند

فصل۳ : نقش توان مصرفی جهت حمله آنالیز توان

فصل۴ : مبانی حملات آنالیز توان

فصل ۵: روش حمله آنالیز توان و ارائه نتایج

فصل۱: پیشگفتار

۱-۱) مقدمه:

امروزه اطلاعات پزشکی برای هر فرد بسیار حیاتی است، اما دسترسی سریع، به موقع و آسان به این اطلاعات اهمیت بیشتری دارد. مسلما با شیوه سنتی دسترسی به این اطلاعات مشکلات بسیاری را در پی دارد. علاوه بر این در شیوه سنتی امکان مفقود شدن اطلاعات بسیار زیاد می باشد که برای جلوگیری یا به عبارتی از بین بردن این مشکلات می توان از تکنولوژی کارت های هوشمند استفاده کرد. با استفاده از کارت های هوشمند می توان اطلاعات پزشکی هر فرد را به سرعت بازیابی کرد و پزشک مربوطه می تواند با توجه به اطلاعات پزشکی قبلی بیمار برای وی بهتر و ساده تر تصمیم گیری کند.

تاکنون اکثر کشورها در بخش پزشکی خود به سمت استفاده از کارت های هوشمند، گرایش پیدا کرده اند. با استفاده از کارت سلامت می توان اطلاعات فردی، پزشکی و درمانی بیمار را ذخیره نمود و در مراکز مشخص از آنها استفاده کرد. در واقع کارت سلامت، کارت هوشمندی است که موجب تسهیل در درمان بیمار می گردد. البته نقش کارت سلامت در مراقبت های پزشکی اورژانس که امکان دسترسی سریع به اطلاعات و یا امکان برقراری ارتباط با بیمار نیز وجود ندارد، بسیار پر رنگ تر می شود. در کارت هوشمند سلامت می توان با توجه به حجم کارت اطلاعات مختلفی ذخیره نمود، برای نمونه در این

کارت ها علاوه بر موارد گفته شده نظیر اطلاعات پزشکی و فردی می توان اطلاعات دیگری چون اطلاعات بیمه ای بیمار را نیز ذخیره کرد. از کارت های هوشمند سلامت می توان در بخش های مختلف پزشکی استفاده نمود. یک پزشک می تواند برای بیماران خود کارت سلامت صادر کند تا توسط آن به اطلاعات بیماران دسترسی پیدا کند، همچنین در بسیاری از هزینه های جانبی خود از جمله هزینه سندهای کاغذی، می تواند صرفه جویی داشته باشد. پزشک می تواند با استفاده از این کارت به داروها و سوابق درمانی بیمار دسترسی پیدا کرده و با استفاده از این اطلاعات علاوه بر دسترسی به سوابق بیمار از انجام مجدد آزمایش ها، تداخل داروها و... جلوگیری می کند. علاوه بر پزشک ، درمانگاه ها، مراکز خدمات درمانی و حتی بیمارستان ها نیز می توانند از این کارت ها استفاده نمایند تا خدمات درمانی خود را به نحوه مطلوبی به بیماران ارائه کنند.

مزایای کارت سلامت را می توان به دو دسته مزایا از دیدگاه پزشک (بیمارستان، بیمه و...) و مزایا از دیدگاه بیمار تقسیم نمود.

- **مزایای کارت هوشمند سلامت از دیدگاه پزشک (بیمارستان، درمانگاه و...)**:

۱) دسترسی سریع و آسان به پرونده پزشکی بیمار برای تشخیص سریع و درست.

۲) تسهیل و تسریع در امر پرداخت های سازمان به پزشکان و مراکز خدماتی دیگر.

۳) دسترسی فوری به اطلاعات حیاتی بیمار در هنگام حوادث.

۴) خوانا بودن نسخها.

۵) سهولت در فرآیند تعیین هویت و اعتبار بیمه شده.

- **مزایای کارت هوشمند سلامت از دیدگاه بیمار**

۱) کاهش هزینه های پزشکی.

۲) عدم تکرار آزمایشات.

۳) کاهش اشتباهات در تشخیص و درمان.

۴) کاهش اشتباهات در تجویز دارو برای بیماران خاص.

۵) امکان جابجایی راحت تر نسبت به دفترچه و همیشه همراه داشتن آن.

۶) کاهش اشتباهات در تحویل و مصرف دارو.

۷) امنیت بیشتر اطلاعاتی نسبت به دفترچه.

۸) ارتقای سطح سلامت جامعه.

۹) افزایش کیفیت درمان.

۱۰) کاهش مراجعه غیر ضروری به پزشک و انجام آزمایشات.

۱۱) تسریع درمان در موارد اورژانسی.

۱۲) دسترسی پزشک معالج به سوابق پزشکی بیمار.

کارتهای هوشمند از جمله متداول ترین و در عین حال حساسترین ابزارهای تصدیق کاربر و ذخیره مطمئن اطلاعات سری هستند. در سال ۲۰۰۶ حدود دو میلیارد کارت هوشمند در سراسر دنیا فروخته شده و این بازار هم اکنون نیز بسرعت در حال گسترش است. از اینرو محافظت از این کارتها در مقابل انواع حملات از جمله موضوعات بسیار مهم در حوزه امنیت بشمار می رود. حملات کانال جانبی حملاتی هستند که از اطلاعات کانال جانبی استفاده می کنند. اطلاعات جانبی از سخت افزار در حال پردازش و رمز کردن داده ها بدست می آید و ارتباط چندانی با متن آشکار ورودی یا متن رمز شده معادل آن ندارد. این گونه حملات مورد علاقه بسیاری هستند زیرا در مدت زمانی کوتاه و هزینه کم توسط ابزارهای موجود در یک آزمایشگاه مدرن الکترونیک قابل انجام هستند. هنگامی که سخت افزار در حال پردازش و رمز کردن اطلاعات است می توان از اطلاعاتی نظیر توان مصرفی، تشعشعات الکترو مغناطیسی یا زمان اجرای الگوریتم استفاده کرده و با کمک آنالیزهای آماری و سایر تکنیکهای رمز شکنی کلید رمز نگاری را بدست آورد[1]. بطور کلی و از دیدگاه آکادمیک چنانکه در [2] نشان داده

شده است، کل حالت درونی یک سیستم رمزنگاری مقادیر و نتایجی هستند که هرگز بطور مستقیم در خروجی ظاهر نمی گردند. حملات کانال جانبی بدنبال استفاده از اطلاعات حالت درونی سیستم رمزنگاری هستند و از وابستگی حالت درونی وکلید استفاده کرده یا قسمتی از کلید را مستقیما حدس زده یا آن را با استفاده از مدلهای آماری بدست می آورد. هر نوع بی دقتی در پیاده سازی، بآ سانی الگوریتم را در معرض چنین حملاتی قرار داده که در برخی موارد بسیار خطرناک تر از حملات کلاسیک هستند[3, 4] .

۲-۱) دسته بندی حملات کانال جانبی:

ادبیات رمز نگاری حملات کانال جانبی را به دو دسته عمده و متعامد بر یکدیگر تقسیم بندی می کند[1].

الف)حملات مهاجم و غیر مهاجم :

حملات مهاجم حملاتی هستند که لازمه آن برداشتن پوشش تراشه رمزنگاری و دسترسی مستقیم به اجزائ آن است. یک نوع مثال می تواند وصل کردن سیم به گذرگاهای داده تراشه و مشاهده اطلاعات رد و بدل شده از آن باشد. حملات غیر مهاجم از اطلاعات در دسترس خارجی مانند تشعشعات الکترومغناطیس[19, 20, 21]، توان مصرفی تراشه[22] یا زمان اجرای الگوریتم[18] استفاده می کند.

ب) حملات فعال و غیر فعال :

حملات فعال سعی در کشف کلید رمز از طریق بر هم زدن عملکرد عادی آن دارد. در حالیکه حملات غیر فعال سعی در بدست آوردن اطلاعات از کارت هوشمند در حالت کارکرد عادی آن دارند.

از این منظر میتوان حملات کانال جانبی را به چند دسته عمده تقسیم بندی نمود.

۱) حمله پروب گذاری.

۲) حمله القائ خطا.

۳) حمله تحلیل زمانی.

۴) حمله تحلیل توان.

- **حمله تحلیل توان:**

توان مصرفی تراشه رمزنگاری ممکن است مشخص کند چه عملیاتی در حال اجرا است و اطلاعاتی را در مورد عملوندها که کلید یا بیت های مرتبط با آن هستند فاش کند زیرا نوعی همبستگی میان توان مصرفی و دستور العملهای اجرا شده توسط سیستم رمزنگاری وجود دارد ایده حمله به سیستم های رمزنگاری با استفاده از توان مصرفی آنها اولین بار توسط P.Kocher مطرح شد[5] . حمله آنالیز توان به دو دسته عمده حمله آنالیز توان ساده و تفاضلی تقسیم می شود.

- **حمله آنالیز توان تفاضلی** :

حمله آنالیز توان تفاضلی یک نوع از حمله های کانال جانبی (حمله تحلیل توان) می باشد در این نوع حمله دیتاهای ورودی به وسیله رمز نگاری ارسال می شود و موقعیکه وسیله رمز نگاری در حال رمز نگاری است توان مصرفی آن نمونه برداری می شود. پس از جمع آوری نمونه های توان به ازای ورودی های متفاوت توان مصرفی وسیله رمز نگاری را باید مدل نمود. لازم نیست تمام جزیات وسیله رمز نگاری را مدل نمود بلکه می توان از مدل همینگ که در فصل آینده توضیح خواهیم داد استفاده نمود و توان مصرفی فرضی را بدست آورد. سپس داده های ورودی که به وسیله رمز نگاری ارسال گردید را به مدل توان فرضی وسیله رمز نگاری ارسال می نماییم و توان فرضی را به ازاء هر ورودی و با قسمتی از کلید که به صورت تغیر کل فضای حالت، تغییر می نماید را بدست می آوریم و این نمونه های توان فرضی را با نمونه های توان اندازه گیری شده مقایسه می کنیم و در هر کجا که بیشترین شباهت را داشته قسمتی از کلید صحیح استخراج می گردد و به سراغ قسمت دیگر کلید می رویم.

در این پایان نامه در ابتدا به بحث در مورد الگوریتم رمز نگاری پرداخته میشود و روش های مختلف رمز نگاری از جمله رمز نگاریAES مورد شرح قرار گرفته است. همچنین مروری اجمالی بر کارتهای هوشمند و سیستم رمز نگاری و احراز هویت در

کارت هوشمند مورد بررسی قرار گرفته است. در مورد کارت هوشمند RFID و احراز هویت آن نیز با ذکر مثال توضیح داده شده است. در فصل سوم به معرفی توان مصرفی وسایل رمز نگاری و مدارات دیجیتال پرداخته است زیرا جهت حمله آنالیز توان مدل سازی توان مصرفی وسیله رمز نگاری بسیار مهم است در این فصل مدل ضریب همینگ جهت مدل کردن توان مصرفی تشریح شده است. وسایل مورد نیاز جهت اندازه گیری توان مصرفی کارتهای هوشمند RFID مورد بررسی قرار گرفته است. جهت اندازه گیری توان الکترومغناطیسی تشعشعی چیپ جهت حمله آنالیز توان راهکارهایی ارئه شده است. در فصل چهارم حمله آنالیز توان مورد بحث قرار گرفته است این حمله که حمله بسیار مهم وکار آمدی است و با پردازش بر روی نمونه های توان اندازه گیری شده از وسیله رمز نگاری و مقایسه با نمونه های مدل شده به ازای کلیدهای مختلف می تواند کلید مخفی را بدست آورد. در این فصل مفصل حمله آنالیز توان تفاضلی مورد بحث قرار گرفته است. در فصل پنجم به آزمایشها و نتایج پیاده سازی ها پرداخته است. در این پروژه در ابتدا بر روی یک میکروکنترلر الگوریتم رمز نگاری پیاده شده البته با کلید یک بایتی و کلید صحیح توسط حمله آنالیز توان با نمونه برداری از توان مصرفی توانستیم به AES حمله کنیم و کلید صحیح را استخراج کنیم و در مرحله بعدی کلید را ۱۶بایتی در نظر گرفتیم و دوباره حمله را انجام دادیم که کلید صحیح را نیز استخراج کردیم. در قسمت بعدی حمله بر روی RFID صورت گرفت البته در این آزمایش نمونه های توان از مرکز تحقیقاتی واقع در استرلیا اخذ گردید و حمله آنالیز توان برروی RFID در حالتهای مختلف انجام گرفت وکلید صحیح استخراج گردید. در مرحله بعدی توان مصرفی یک میکروکنترلر که الگوریتم رمز نگاری را اجرا میکرد و توسط نرم افزار ساده وکارآمد PROTEUS شبیه سازی گردید و نمونه های توان به نرم افزار متلب ارسال گردید سپس در مرحله بعدی این مدلسازی جهت پیاده سازی ضد حمله هایی مثل مخفی سازی و ماسک گزاری تست گردید و یک نمونه مخفی سازی و ماسک گزاری بر روی یک میکروکنترلر بیان گردید و دوباره به آن حمله آنالیز توان صورت گرفت و نشان دادیم که با وجود ضد حمله هامی توان دوباره به آن حمله نمود. در ادامه جمع بندی و پیشنهادات جهت ادامه کار ارائه گردیده است.

دراین پایان نامه حمله آنالیز توان به کارتهای هوشمند و مخصوصاً کارتهای هوشمند RFID مورد بررسی قرار گرفته است و همچنین چگونگی خنثی کردن این حمله ها نیز شرح داده شده است.

فصل۲: معرفی الگوریتم رمز نگاری وکارت هوشمند

۲-۱)کلیات وچارچوب رمز نگاری:

رمز نگاری عبارت است از یک نظام یا الگوی ریاضی/منطقی که بر اساس آن اطلاعات و مفاهیم آشکار و قابل فهم برای همگان طبق روالی برگشت پذیر به اطلاعاتی نامفهوم و گنگ تبدیل می شود. این اطلاعات نا مفهوم و گنگ توسط کسی که روال معکوس و پارامترهای لازم را می داند قابل برگشت و بهره برداری است. طبق اصل کرکهف چون قرارنیست هیچ نکته ای در بطن الگوریتم رمزنگاری و روال معکوس آن(یعنی رمز گشایی)مخفی بماند لذا در تمام الگوریتم های رمزنگاری به پارامتری به نام کلید رمز احتیاج است. که با تغییرآن ماهیت گنگ و مبهم اطلاعات رمز شده به نحو غیر قابل پیش بینی تغییرمی کند. لذامی توان فرایندرمز نگاری را تابعی به شکل زیر تصور کرد:

$$c = f(p, k)$$

p: پیامی است که باید رمزگذاری شود p را متن آشکار[۱] می گویند.

k: پارامتری که متن آشکار براساس مقدار آن به نحو غیر قابل پیش بینی و مبهم و درهم و بی معنی می شود پارامتر k به کلید رمز شهرت دارد.

---

[۱] Plain Text

c: حاصل فرایند رمزنگاری p با کلید k و تابع f قطعه ای اطلاعات بی معنی موسوم به متن رمز[۲] است.

به طور خلاصه: رمز نگاری مسئله سری نگه داشتن یک پیام با طول بزرگ و دلخواه را به مسئله سری نگه داشتن یک کلید کوتاه کاهش می دهد. سیستم های رمز نگاری به دو رده کلی رمز نگاری متقارن و رمز نگاری کلید عمومی تقسیم بندی می شوند.

۱-۱-۲)رمزنگاری متقارن:

در رمز نگاری متقارن، رمز نگاری، ورمز گشایی اطلاعات باکلیدی مشابه صورت می گیرد این کلید باید بین طرفین ارتباط توافق شده باشد. از ویژگی کلی سیستم های رمز نگاری متقارن می توان به موارد ذیل اشاره کرد.

الف) سیستم ها و الگوریتم های رمز نگاری متقارن از لحاظ عملکرد بسیارسریع اند و امکان پیاده سازی سخت افزاری و نرم افزاری آن برای رمز نگاری بی درنگ داده ها تا نرخ بالاتر از گیگا بایت برثانیه وجود دارد.

ب) در رمزنگاری متقارن داده های متن اصلی در قالب های بلوک هایی با طول ثابت و عموماً کوتاه (۶۴-۱۲۸یا ۲۵۶ بیتی) پردازش و رمز می شوند.

ج) چون کلیدهای رمزنگاری و رمز گشایی مشابه یکدیگرند لذا طرفین ارتباط باید به روش مطمئن (مثلاً از طریق ملاقات حضوری یا شخصی معتمد و یا سیستمی خودکار ولی مطمئن)کلید خود را توافق کرده و از آن بهره بگیرند. امنیت کلی داده ها به امنیت کلید گره خورده است.

د) هرگاه شخص یا سرویس دهنده ای بتواند با تعداد زیادی از کاربران ارتباط امن و رمز نگاری شده داشته باشد باید با تک تک آنها کلیدی مجزا و مستقل را توافق کند چرا که تعریف کلیدی واحد برای همه کاربران اول امکان استراق سمع کاربران از اطلاعات یکدیگر رافراهم می آورد ثانیا سهل انگاری یاخیانت یکی از کاربران امنیت تمام آنها را به خطرخواهد انداخت.

---

[۲] Cipher Text

ه) عموما درتمام روش های رمز نگاری متقارن فرایند ادغام داده ها وکلید هرگونه عملیات درهم ریختن داده ها چندین بارتکرار میشود. به تکرار هر بار از این عملیات دور[۳] گفته می شود تعداد دورها بین ۸ تا۶۴ دورتغییرمی کند.

و) درسیستم های رمز نگاری متقارن عموما فرایند رمز گشایی و رمز نگاری تشابه کامل دارند با این تفاوت که فقط مقادیر متغیرها و ثابت ها عوض می شوند ولی در مجموع ذات ساختار الگوریتم رمز نگاری و رمز گشایی متحدالشکل و یکسان است.

ز) درشبکه ای که جمعاً N کاربر وجود دارد و دو به دوی آنها می خواهند با یکدیگر ارتباط امن و رمز نگاری شده برقرار کنند به تعریف و توافق $n\frac{(n-1)}{2}$ کلید سری و متقارن نیاز است.

روشهای رمز نگاری متقارن و مدرن مانند روش RC6-Serpent-IDEA-3DES-AES-DES می باشند.

۲-۱-۲) رمز نگاری کلید عمومی:

قفلی را مجسم که دارای دو کلید سبز و قرمز است کلید سبز فقط در جهت ساعت گرد می چرخد و صرفا می تواند آن را قفل کند ولی وقتی قفل بسته شد فقط می توان کیلد سبز را خارج کرد. چون به هیچ وجه درسمت پاد ساعتگرد نخواهد چرخید. چنین کلیدی را می توان به تعداد فراوان تکثیر کرد و در اختیار دوست و دشمن گذاشت چرا که با این کلید فقط می توان قفل را بست و قفل بسته را باز نخواهد کرد. درسمت مقابل کلید قرمز فقط درسمت پاد ساعتگرد و برای گشودن قفل می چرخد این کلید نزد صاحب قفل می ماند و به وسواس از آن مراقبت می شود تجسم چنین قفلی در دنیای مجازی با الگوریتم رمز نگاری کلید عمومی تحقق یافته است. در الگوریتم های رمز نگاری کلید عمومی، دو پارامتر به عنوان کلید عمومی وکلید خصوصی تعریف شده که با کلید عمومی می توان داده ها را رمز نگاری کرد و داده های رمز نگاری شده را نمی توان باچنین کلیدی از رمز خارج کرد. پارامترکلید عمومی را می توان به راحتی در اختیار همگان قرار داد و یا آن را از

---

[۳] Round