





دانشکده فنی و مهندسی

بخش مهندسی صنایع

گروه مهندسی فناوری اطلاعات

پایان نامه کارشناسی ارشد مهندسی فناوری اطلاعات

طراحی و پیاده سازی نرم‌افزاری مناسب یک الگوریتم

رمزنگاری بلوکی بومی بر روی کارت هوشمند

دانشجو:

یعقوب محمودی

استاد راهنما:

دکتر حمید رضا اسکندری

استاد مشاور:

دکتر علی یزدیان

خرداد ۱۳۸۹

آیین نامه چاپ پایان نامه (رساله) های دانشجویان دانشگاه تربیت مدرس

نظر به اینکه چاپ و انتشار پایان نامه (رساله) های تحصیلی دانشجویان دانشگاه تربیت مدرس، مبین بخشی از فعالیتهای علمی - پژوهشی دانشگاه است بنابراین به منظور آگاهی و رعایت حقوق دانشگاه، دانش آموختگان این دانشگاه نسبت به رعایت موارد ذیل متعهد می شوند:

ماده ۱: در صورت اقدام به چاپ پایان نامه (رساله) ی خود، مراتب را قبلاً به طور کتبی به «دفتر نشر آثار علمی» دانشگاه اطلاع دهد.

ماده ۲: در صفحه سوم کتاب (پس از برگ شناسنامه) عبارت ذیل را چاپ کند:

«کتاب حاضر، حاصل پایان نامه کارشناسی ارشد نگارنده در رشته مهندسی فناوری اطلاعات است که در سال ۸۹ در دانشکده فنی مهندسی دانشگاه تربیت مدرس به راهنمایی جناب آقای دکتر حمید رضا اسکندری و مشاوره جناب آقای دکتر علی یزدیان از آن دفاع شده است.»

ماده ۳: به منظور جبران بخشی از هزینه های انتشارات دانشگاه، تعداد یک درصد شمارگان کتاب (در هر نوبت چاپ) را به «دفتر نشر آثار علمی» دانشگاه اهدا کند. دانشگاه می تواند مازاد نیاز خود را به نفع مرکز نشر در معرض فروش قرار دهد.

ماده ۴: در صورت عدم رعایت ماده ۳، ۵۰٪ بهای شمارگان چاپ شده رابه عنوان خسارت به دانشگاه تربیت مدرس، تأدیه کند.

ماده ۵: دانشجو تعهد و قبول می کند در صورت خودداری از پرداخت بهای خسارت، دانشگاه می تواند خسارت مذکور را از طریق مراجع قضایی مطالبه و وصول کند؛ به علاوه به دانشگاه حق می دهد به منظور استیفای حقوق خود، از طریق دادگاه، معادل وجه مذکور در ماده ۴ را از محل توقیف کتابهای عرضه شده نگارنده برای فروش، تامین نماید.

ماده ۶: اینجانب یعقوب محمودی دانشجوی رشته مهندسی فناوری اطلاعات مقطع کارشناسی ارشد تعهد فوق و ضمانت اجرایی آن را قبول کرده، به آن ملتزم می شوم.

یعقوب محمودی

دستورالعمل حق مالکیت مادی و معنوی در مورد نتایج پژوهشهای علمی دانشگاه تربیت مدرس

مقدمه: با عنایت به سیاست‌های پژوهشی دانشگاه در راستای تحقق عدالت و کرامت انسانها که لازمه شکوفایی علمی و فنی است و رعایت حقوق مادی و معنوی دانشگاه و پژوهشگران، لازم است اعضای هیات علمی، دانشجویان، دانش آموختگان و دیگر همکاران طرح، در مورد نتایج پژوهشهای علمی که تحت عناوین پایان‌نامه، رساله و طرحهای تحقیقاتی که با هماهنگی دانشگاه انجام شده است، موارد ذیل را رعایت نمایند:

ماده ۱- حقوق مادی و معنوی پایان‌نامه‌ها / رساله‌های مصوب دانشگاه متعلق به دانشگاه است و هرگونه بهره‌برداری از آن باید با ذکر نام دانشگاه و رعایت آیین‌نامه‌ها و دستورالعمل‌های مصوب دانشگاه باشد.

ماده ۲- انتشار مقاله یا مقالات مستخرج از پایان‌نامه / رساله به صورت چاپ در نشریات علمی و یا ارائه در مجامع علمی باید به نام دانشگاه بوده و استاد راهنما مسئول مکاتبات مقاله باشد.

تبصره: در مقالاتی که پس از دانش آموختگی بصورت ترکیبی از اطلاعات جدید و نتایج حاصل از پایان‌نامه / رساله نیز منتشر می‌شود نیز باید نام دانشگاه درج شود.

ماده ۳- انتشار کتاب حاصل از نتایج پایان‌نامه / رساله و تمامی طرحهای تحقیقاتی دانشگاه باید با مجوز کتبی صادره از طریق حوزه پژوهشی دانشگاه و بر اساس آئین‌نامه‌های مصوب انجام می‌شود.

ماده ۴- ثبت اختراع و تدوین دانش فنی و یا ارائه در جشنواره‌های ملی، منطقه‌ای و بین‌المللی که حاصل نتایج مستخرج از پایان‌نامه / رساله و تمامی طرحهای تحقیقاتی دانشگاه باید با هماهنگی استاد راهنما یا مجری طرح از طریق حوزه پژوهشی دانشگاه انجام گیرد.

ماده ۵- این دستورالعمل در ۵ ماده و یک تبصره در تاریخ ۱۳۸۴/۴/۲۵ در شورای پژوهشی دانشگاه به تصویب رسیده و از تاریخ تصویب لازم الاجرا است و هرگونه تخلف از مفاد این دستورالعمل، از طریق مراجع قانونی قابل پیگیری می‌شود.

یعقوب محمودی

تقدیم بہ:

✓ پدر و مادر بزرگوارم بہ خاطر ہمہ خوبی ہایشان

✓ ہمسر کرامیم کہ ہمارہ مشوق من بودہ و در طی این دورہ با صبر و تحمل ستودنی خود من را یاری رساندہ.

✓ فرزندان عزیزم (نایہ و محسن)

مشکر و قدردانی از:

✓ استاد گرامی دکتر حمیدرضا اسکندری (استاد راهنمای پایان نامه)

✓ استاد گرامی دکتر علی یزدیان (استاد مشاور پایان نامه)

✓ مهندس مجید سلطانی (معاون فناوری اطلاعات و ارتباطات ناجا)

چکیده

امروزه سامانه‌های مبتنی بر کارت هوشمند به طور گسترده در سراسر دنیا رایج گردیده‌اند. کارت‌های هوشمند در کاربردهایی از قبیل کنترل دسترسی، تجارت الکترونیک، احراز هویت و از این قبیل استفاده می‌گردند. به خاطر اهمیت این کاربردها، ملاحظات امنیتی برای تولید کنندگان و کاربران کارت هوشمند حیاتی است. استفاده کنندگان وقتی می‌توانند در یک فرآیند امن از خدمات مبتنی بر کارت‌های هوشمند بهره‌گیرند که حداقل همه مخاطرات امنیتی در بکارگیری آنها را دانسته و برای مقابله با آنها تمهیدات لازم را تدارک دیده باشند.

در این پژوهش ضمن آشنایی با ساختار سخت‌افزاری و نرم‌افزاری کارت‌های هوشمند، مخاطرات امنیتی آنها شناسایی و استفاده از رمزنگاری بعنوان یکی از روشهای اصلی مقابله با این مخاطرات مورد بررسی قرار خواهد گرفت. عملیات رمزنگاری بر مبنای یک الگوریتم رمز انجام می‌گیرد. الگوریتم‌های رمز با روشهای سخت‌افزاری یا نرم‌افزاری پیاده‌سازی و قابل بکارگیری می‌باشند.

در این پایان نامه الگوریتم رمز AES با ساختار تغییر یافته، بعنوان الگوریتم رمز بومی در نظر گرفته شده و بصورت نرم‌افزاری بر روی کارت هوشمند TOP-IMGX4 ساخت شرکت Gemalto پیاده‌سازی و با پیاده‌سازی‌های نرم‌افزاری الگوریتم AES که بر روی میکروکنترلر ATMega163 و میکروکنترلر ۸۰۵۱ انجام شده است و همچنین پیاده‌سازی‌های سخت‌افزاری الگوریتم AES که بر روی تراشه FPGA مدل XC2S515-6 و کارت هوشمند TOP-IMGX4 انجام گردیده، مقایسه شده است. نتایج حاصله نشانگر آن است که پیاده‌سازی نرم‌افزاری الگوریتم رمز بومی برای همه کاربردهای غیر بلادرنگ مناسب بوده اما برای کاربردهای بلادرنگ صرفاً با افزایش منابع پردازشی و حافظه کارت هوشمند قابل استفاده خواهد بود.

کلید واژه: امنیت اطلاعات، کارت هوشمند، حملات امنیتی، مخاطرات امنیتی، الگوریتم رمزنگاری

فهرست مطالب

فصل اول - معرفی و کلیات	۱
۱-۱-مقدمه	۱
۱-۲- ضرورت پژوهش	۴
۱-۳- تعریف مسئله	۵
۱-۴- جنبه جدید بودن و نوآوری	۵
۱-۵- تعاریف و اصطلاحات	۶
۱-۶- ساختار پایان نامه	۶
۱-۷- خلاصه فصل	۷
فصل دوم- ساختار کارت هوشمند	۸
۲-۱- مقدمه	۸
۲-۲- کارت هوشمند چیست؟	۹
۲-۳-انواع کارت از نظر روش ارتباط با دنیای بیرون	۱۰
۲-۴-اجزای کارت	۱۰
۲-۴-۱- اجزاء کارت هوشمند تماسی	۱۱
۲-۴-۲- اجزاء کارت هوشمند غیر تماسی	۱۲
۲-۵- دستگاه کارت خوان	۱۳
۲-۵-۱- کارت خوانهای تماسی	۱۴
۲-۵-۲- کارت خوان های غیرتماسی	۱۴
۲-۵-۳- کارت خوان های ترکیبی	۱۵
۲-۶- معماری تراشه کارت هوشمند	۱۵
۲-۷- مراحل ساخت سخت افزار کارت هوشمند	۱۷
۲-۸- نرم افزارهای کارت هوشمند	۱۸
۲-۹- انواع سیستم عامل در کارت های هوشمند	۱۹

۱۹	۲-۹-۱. کارت‌های Open-OS
۲۰	۲-۹-۲. کارت‌های بومی
۲۰	۲-۱۰. برنامه‌های کاربردی
۲۰	۲-۱۱. ساختار منطقی فایل‌های درون کارت
۲۲	۲-۱۲. خلاصه فصل
۲۳	فصل سوم - مخاطرات امنیتی کارت هوشمند
۲۳	۳-۱. مقدمه
۲۴	۳-۲. امنیت کارت هوشمند
۲۵	۳-۳. دسته‌بندی حملات
۲۷	۳-۴. حملات در سطح فیزیکی
۲۸	۳-۴-۱. تحلیل ایستا تراشه کارت هوشمند
۲۹	۳-۴-۲. تحلیل پویا تراشه کارت هوشمند
۲۹	۳-۵. حملات در سطح منطقی
۳۰	۳-۵-۱. استفاده از کارت‌های هوشمند جعلی
۳۰	۳-۵-۲. تعیین مجموعه فرمان‌های یک کارت هوشمند
۳۰	۳-۵-۳. شنود داده‌های در حال نقل و انتقال
۳۰	۳-۵-۴. حمله به کارت با قطع انرژی الکتریکی
۳۱	۳-۵-۵. تحلیل جریان الکتریکی در مدت تطبیق PIN
۳۱	۳-۵-۶. تحلیل زمانی مقایسه‌های PIN
۳۲	۳-۵-۷. تحلیل توانی ساده و تفاضلی برای بازیابی داده‌ها
۳۲	۳-۶. ایجاد حفاظت با رمزنگاری داده‌ها
۳۲	۳-۷. خلاصه فصل
۳۴	فصل چهارم - ساختار الگوریتم رمز بومی
۳۴	۴-۱. مقدمه
۳۵	۴-۲. تشریح عملیات رمزنگاری
۳۹	۴-۳. اهمیت جعبه‌های جایگزینی در سیستم‌های رمزنگاری قالبی

۴۰	۴-۴. جعبه جایگزینی بومی
۴۲	۵-۴. خلاصه فصل
۴۳	فصل پنجم - پیاده‌سازی الگوریتم رمز بومی
۴۳	۱-۵. مقدمه
۴۴	۲-۵. مراحل پیاده‌سازی نرم‌افزاری الگوریتم رمز بومی
۴۶	۳-۵. مشخصات یک پیاده‌سازی مناسب نرم‌افزاری الگوریتم رمز بر روی کارت هوشمند
۴۷	۱-۳-۵. راستی‌آزمایی پیاده‌سازی منطقی الگوریتم رمز
۴۷	۲-۳-۵. بهینه نمودن پیاده‌سازی نرم‌افزاری برای بهبود عملکرد اجرایی الگوریتم رمز
۵۴	۳-۲-۵. مقاوم نمودن نرم‌افزار الگوریتم در برابر کدهای مخرب و حملات کانال جانبی
۶۷	۴-۵. نتایج نهایی پیاده‌سازی نرم‌افزاری الگوریتم رمز بومی
۶۹	۵-۵. خلاصه فصل
۷۱	فصل ششم - ارزیابی پیاده‌سازی الگوریتم رمز بومی
۷۱	۱-۶. مقدمه
۷۲	۲-۶. بررسی چند نمونه پیاده‌سازی الگوریتم رمز AES
۷۳	۳-۶. مقایسه پیاده‌سازی انجام شده در این تحقیق با نمونه پیاده‌سازی‌های فوق
۷۶	فصل هفتم - نتیجه‌گیری و جمع‌بندی
۷۶	۱-۷. مقدمه
۷۷	۲-۷. مروری بر فصل‌های گذشته
۷۷	۳-۷. دستاوردهای پژوهش
۷۷	۴-۷. نوآوری‌های پژوهش
۷۸	۵-۷. نقاط قوت و ضعف پیاده‌سازی انجام شده
۷۸	۶-۷. افق‌های پژوهشی آینده
۷۹	۷-۷. خلاصه فصل
۸۰	فهرست منابع :

فهرست شکل ها

- شکل ۱-۲: شکل ظاهری کارت هوشمند..... ۹
- شکل ۲-۲: اجزای تشکیل دهنده کارت هوشمند تماسی..... ۱۱
- شکل ۳-۲: اجزای تراشه کارت هوشمند تماسی..... ۱۲
- شکل ۴-۲: اجزا تشکیل دهنده یک کارت هوشمند غیرتماسی..... ۱۳
- شکل ۵-۲: چند نمونه کارت خوان تماسی..... ۱۴
- شکل ۶-۲: شمای ارتباط یک کارت هوشمند غیرتماسی و نحوه ارتباط با کارت خوان..... ۱۵
- شکل ۷-۲: شمای کلی معماری تراشه در یک کارت هوشمند..... ۱۶
- شکل ۸-۲: مراحل تولید سخت افزار کارت هوشمند..... ۱۸
- شکل ۹-۲: ساختار منطقی فایل های درون یک کارت هوشمند نمونه..... ۲۱
- شکل ۱-۳: رده بندی اجزا امنیت کارت هوشمند..... ۲۴
- شکل ۲-۳: دسته بندی نقاط حمله در تراشه کارت هوشمند در سطح فیزیکی..... ۲۷
- شکل ۱-۴: نمایش بلوک ورودی ۱۲۸ بیتی به صورت آرایه حالت..... ۳۵
- شکل ۲-۴: روند نمای کلی عملیات رمزنگاری..... ۳۶
- شکل ۳-۴: فرآیند جایگزینی بایتها..... ۳۶
- شکل ۴-۴: جعبه جایگزینی (جدول SBox) مربوط به فرایند رمزنگاری..... ۳۷
- شکل ۵-۴: شیفت دادن سطرها..... ۳۷
- شکل ۶-۴: فرآیند ترکیب کردن ستونها..... ۳۸
- شکل ۷-۴: فرآیند اضافه کردن کلید دور..... ۳۹
- شکل ۸-۴: جعبه جایگزینی بومی برای رمزنگاری..... ۴۱

شکل ۴-۹: جعبه جایگزینی بومی برای رمزگشایی ۴۱

شکل ۵-۱: روند نمای تهیه برنامه در جاوا کارت ۴۶

شکل ۵-۲: معماری کلان الگوریتم رمز بومی به صورت UML ۴۹

فهرست جدول ها

جدول ۵-۱: مشخصات تراشه کارت هوشمند مورد استفاده ۶۸

جدول ۵-۲: مختصات و مشخصه‌ها جاوا کارت مورد استفاده ۶۹

جدول ۵-۳: نتایج پیاده‌سازی و اجرای الگوریتم رمزنگاری بومی ۷۰

جدول ۶-۱: مقایسه نتایج پیاده‌سازی و اجرای الگوریتم رمزنگاری بومی با پیاده‌سازی های دیگر ۷۴

فصل اول

معرفی و کلیات

۱-۱. مقدمه

گسترش فناوری‌های نوین اطلاعاتی و ارتباطی و نفوذ هر چه بیشتر آنها به جامعه باعث ایجاد تغییراتی در روند جاری فرآیندهای مختلف کاری می‌گردد. کارت هوشمند یکی از این فناوری‌ها بوده که در اواسط دهه میلادی ۱۹۷۰ اختراع گردید لیکن تا چندین سال استفاده از آن فراگیر نشده و بطور جدی از اوایل دهه ۱۹۹۰ میلادی در کاربردهای عمومی مورد استفاده قرار گرفت. در دهه گذشته کشورهای مختلف مخصوصاً

کشورهای دارای زیرساختهای لازم از کارت های هوشمند در امور مختلف استفاده نموده و با کمک آنها فرآیندهای ایمنی را، برای خدمات رسانی مطمئن تر بکار گرفتند.

کاربردهای کارت هوشمند بسیار گسترده می باشند . نمونه هایی از این کاربردها عبارتند از :

- کاربردهای مالی^۱
- کارت های اعتباری^۲
- کیف پول الکترونیکی
- کارت های بانکی
- کارت های شناسایی
- گواهینامه رانندگی الکترونیکی
- کنترل تردد
- کنترل دسترسی^۳
- کارت ملی
- مخابرات و رایانه
- کارت های تلفن عمومی

^۱ Financial

^۲ Credit/Debit

^۳ Access Control

- سیم کارت تلفن همراه
- تلویزیون پولی^۴
- اعمال امضای دیجیتال بر روی شبکه های رایانه ای
- قفل های سخت افزاری برای حفاظت از برنامه های رایانه ای
- پرونده پزشکی
- کارت بهداشت
- کارت بیمه
- کارت سلامت
- حمل و نقل
- کارت سوخت
- بلیط مترو، اتوبوس و قطار
- پروازهای هوایی بدون بلیت
- گذرنامه الکترونیکی
- ویزای الکترونیکی

امروزه روند استفاده از کارتهای هوشمند به سرعت در حال افزایش است. بطوریکه در ایران طی چند سال اخیر چندین خدمت عمومی نظیر بعضی از خدمات بانکی، کارت سوخت خودروها، کارتهای شناسایی، گذرنامه الکترونیکی، گواهینامه الکترونیکی، کارت معافیت از خدمت سربازی و . . . با استفاده از کارتهای هوشمند در حال ارائه بوده و چندین خدمت دیگر نظیر کارت ملی الکترونیکی، کارت سلامت، شناسنامه الکترونیکی و چندین خدمت دیگر در آینده نزدیک به این خدمات اضافه می‌شوند. اما بکارگیری گسترده کارتهای هوشمند برای ارائه خدمات مختلف در کشور بدون توجه به موضوع امنیت آن نه تنها کمکی به سازمانهای ارائه دهنده خدمات و مردم نخواهد کرد بلکه در آینده باعث چالشهای جدی خواهد شد. لذا موضوع امنیت کارتهای هوشمند و مخاطرات احتمالی بکارگیری آنها از اهمیت ویژه‌ای برخوردار است.

۱-۲. ضرورت پژوهش

کارتهای هوشمند نیز نظیر دیگر فناوریهای اطلاعاتی و ارتباطی به یک سری اقدامات امنیتی نیازمند هستند، که با رعایت آنها امکان بکارگیری روشهای امن در ارائه خدمات مبتنی بر کارت هوشمند ممکن خواهد شد. این اقدامات امنیتی بدلیل سعی و تلاش عده‌ای برای رخنه در سامانه های مبتنی بر کارتهای هوشمند بطور مداوم در حال تغییر و به روز شدن می‌باشند. در این پژوهش ابتدا مخاطرات امنیتی کارتهای هوشمند شناسایی و سپس روشهای امن‌سازی کارتهای هوشمند بررسی خواهد شد. از جمله اقدامات مهم برای امن‌سازی کارتهای هوشمند، رمزنگاری اطلاعات ذخیره شده بر روی کارت و همچنین مبادله امن اطلاعات بین کارت هوشمند و فضای بیرونی است. این اقدام از دستیابی افراد غیر مجاز به اطلاعات مهم جلوگیری نموده و بسیاری از مخاطرات را که رخنه‌گر نهایتاً هدفی جز دستیابی به اطلاعات ندارد را مرتفع می‌نماید. رمزنگاری اطلاعات بر پایه یک الگوریتم رمزنگاری امکان پذیر بوده و هر چه الگوریتم رمز بکار گرفته شده قوی‌تر باشد امکان انجام رمزنگاری مطمئن‌تری وجود خواهد داشت. اما از آنجائیکه کارتهای هوشمند برای کاربردهای مختلف و از جمله کاربردهای به هنگام استفاده می‌گردند لذا سرعت اجرای عملیات رمزنگاری نیز از اهمیت ویژه‌ای برخوردار است. این موضوع با در نظر گرفتن منابع محدود پردازشی و حافظه‌ای موجود بر روی کارت هوشمند بیشتر خودنمایی نموده و پیاده‌سازی الگوریتم‌های رمزنگاری را با

محدودیت مواجه می‌نماید. در بسیاری از کاربردهای عمومی و تجاری از الگوریتمهای رمزنگاری استاندارد نظیر DES و AES استفاده می‌گردد لیکن در کاربردهای خاص دولتی و نظامی برای استفاده از الگوریتمهای رمزنگاری استاندارد و عمومی محدودیت وجود داشته و از الگوریتمهای اختصاصی و بومی استفاده می‌شود.

۳-۱. تعریف مسئله

در کارتهای هوشمند پیاده‌سازی الگوریتمهای رمزنگاری به دو صورت سخت افزاری و نرم‌افزاری امکان‌پذیر است. پیاده‌سازی سخت‌افزاری الگوریتم رمزنگاری در یک کارت هوشمند مستلزم در اختیار داشتن امکانات لازم برای طراحی تراشه‌های الکترونیکی و از آن مهمتر در اختیار داشتن کارخانه‌های تولید تراشه الکترونیکی است. اما پیاده‌سازی نرم‌افزاری با محدودیتهای کمتری مواجه بوده و با در اختیار داشتن کارتهای هوشمند و ابزارهای نرم‌افزاری و سخت‌افزاری مورد نیاز امکان‌پذیر خواهد بود. در حال حاضر در داخل کشور کارخانه تولید تراشه‌های الکترونیکی وجود نداشته و پس از طی مراحل طراحی تراشه باید ادامه فرآیند تولید تراشه در خارج از کشور دنبال گردد که این موضوع با محدودیتهای قانونی مواجه است. زیرا در پیاده‌سازی یک الگوریتم رمز بومی برای کاربردهای خاص انتشار مشخصات الگوریتم رمز با محدودیتهای قانونی مواجه بوده و باید کل فرایند پیاده‌سازی در داخل کشور انجام گردد. از این رو پیاده‌سازی نرم‌افزاری الگوریتم رمز بومی بعنوان موضوع این پژوهش انتخاب گردیده است.

۴-۱. جنبه جدید بودن و نوآوری

در حال حاضر صرفاً الگوریتمهای رمزنگاری استاندارد بصورت سخت‌افزاری و بر روی بعضی از کارتهای هوشمند در دسترس می‌باشد که بنا بر دلائل ارائه شده در قسمت قبل در همه کاربردها قابل استفاده نمی‌باشند. در این پژوهش یک الگوریتم رمز بومی بصورت نرم‌افزاری بر روی یک کارت هوشمند پیاده‌سازی شده و شرایط لازم برای دستیابی به مناسب‌ترین حالت پیاده‌سازی از جهت عملکرد منطقی، سرعت اجرا و امنیت برنامه‌نویسی بررسی خواهد شد.

۵-۱. تعاریف و اصطلاحات

امنیت اطلاعات : امنیت اطلاعات، فرآیند حفاظت از داده برای ممانعت از دسترسی و استفاده غیر مجاز، فاش شدن، تخریب و تغییر داده می‌باشد (ذاکرالحسینی، ۱۳۸۶).

حمله : نقض یکی از سرویس‌های امنیتی پنجگانه محرمانگی، احراز هویت، صحت، کنترل دسترسی و در دسترس بودن (ذاکرالحسینی، ۱۳۸۶).

مهاجم / نفوذگر / رخنه کننده : شخص یا سازمانی که از دانش خود برای نفوذ به یک سامانه و دسترسی غیر مجاز به اطلاعات و یا خرابکاری استفاده می‌کند .

حملات امنیتی : مجموعه اقدامات خرابکارانه برای نفوذ به یک سیستم و یا خدشه وارد نمودن به آن

کارت هوشمند : کارت هایی پلاستیکی با ابعاد مختلف که دارای یک مدار مجتمع^۵ بوده و ابزار مناسبی برای خدمات الکترونیکی در زمینه‌های گوناگون می‌باشند (Chen Z., 2006).

الگوریتم رمز : یک نظام ریاضی و منطقی است که بر اساس آن اطلاعات و مفاهیم آشکار و قابل فهم برای همگان، طبق روالی برگشت پذیر به اطلاعاتی نامفهوم و گنگ تبدیل می‌شود (ذاکرالحسینی، ۱۳۸۶).

۶-۱. ساختار پایان نامه

فصل اول : مقدمه و کلیات

فصل دوم : ساختار افزار کارت هوشمند، نرم‌افزارهای پایه و نرم‌افزارهای کاربردی مورد استفاده در کارتهای هوشمند مورد بررسی قرار خواهد گرفت.

فصل سوم : مخاطرات امنیتی کارتهای هوشمند و انواع حملات شناخته شده تاکنون که بر علیه آنها دسته بندی و بیان شده و برخی از روشهای ایمن سازی در سخت افزار و نرم افزار کارتهای هوشمند مرور می گردد.

فصل چهارم : ساختار الگوریتم رمز بومی مورد نظر برای پیاده سازی بررسی و مشخصات آن بیان می گردد.

فصل پنجم : پیاده سازی نرم افزاری الگوریتم رمز بومی و روشهای بهینه نمودن آن ارائه خواهد شد.

فصل ششم : پیاده سازی نرم افزاری الگوریتم رمز بومی ارزیابی و با چند نمونه پیاده سازی قبلی مقایسه می گردد.

فصل آخر: به نتیجه گیری و جمع بندی موضوعات ارائه شده در فصول قبل پرداخته و موضوع پیشنهادی برای پژوهش های بعدی طرح خواهد شد.

۱-۷. خلاصه فصل

در این فصل برای ارائه کلی پژوهش مقدمه ای ارائه شده است. ضرورت انجام این پژوهش و مسئله تحقیق مطرح گردیده و جنبه های نوآوری آن بیان شده است. در فصل بعد ساختار کارت هوشمند مورد بررسی قرار خواهد گرفت.