
بسم الله الرحمن الرحیم

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:**

دکترحمید رضا اسکندری

**استاد مشاور:**

دکتر علی یزدیان

خرداد ۱۳۸۹

## آیین نامه چاپ پایان‌نامه (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 می‌شوند:

ماده ۱: در صورت اقدام به چاپ پایان نامه (رساله)ی خود، مراتب را قبلاً به طور کتبی به «دفتر نشر آثارعلمی» 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 سال۸۹ 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 هزینه‌های انتشارات دانشگاه، تعداد یک درصد شمارگان کتاب (در هر نوبت‌چاپ) را به «دفتر نشر آثارعلمی» دانشگاه اهدا کند. دانشگاه می‌تواند مازاد نیاز خود را به نفع مرکز نشر درمعرض فروش قرار دهد.

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

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

ماده ۶: اینجانب یعقوب محمودی دانشجوی رشته مهندسی فناوری اطلاعات مقطع‌کارشناسی 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 پایان نامه‌ها / 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 پایان نامه/ 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 پایان نامه / رساله و تمامی طرحهای تحقیقاتی دانشگاه باید با مجوز کتبی صادره از طریق حوزه پژوهشی دانشگاه و بر اساس آئین نامه های 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 پایان نامه/ 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 می شود.

**یعقوب محمودی**

# تقدیم به:

- ✓ پدر و مادر بزرگوارم به خاطر همه خوبی هایشان
- ✓ همسر گرامیم که همواره مشوق من بوده و در طی این دوره با صبر و تحمل ستودنی خود من را یاری رساند.
- ✓ فرزندان عزیزم (هانیه و محسن)

## تشکر 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 بهره گیرند 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 پیاده سازی 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 پیاده سازی و با پیاده‌سازی‌های نرم‌افزاری الگوریتم AES که بر روی میکروکنترلر ATMega163 و میکروکنترلر ۸۰۵۱ انجام شده است و همچنین پیاده‌سازی‌های سخت افزاری 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

# فهرست شکل ها

# فهرست جدول ها

# 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 مطمئن‌تر بکار گرفتند.

کاربردهای کارت هوشمند بسیار گسترده می‌باشند . 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] Finantial

[۲] Credit/Debit

[۳] Access Control

- سیم کارت تلفن همراه
- تلویزیون پولی[۴]
- اعمال امضای دیجیتال بر روی شبکه های رایانه‌ای
- قفل‌های 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

---

[۴] Pay TV1

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 الکترونکی، 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.

## ۱-۳. تعریف مسئله

در کارتهای هوشمند پیاده‌سازی الگوریتم‌های رمزنگاری به دو صورت سخت افـزاری و نـرم‌افـزاری امکان‌پذیر است. پیاده‌سازی سخت‌افزاری الگوریتم رمزنگـاری در یـک کـارت هوشـمند مسـتلزم در اختیـار داشتن امکانات لازم برای طراحی تراشه‌های الکترونیکی و از آن مهمتر در اختیار داشتن کارخانه‌هـای تولیـد تراشه الکترونیکی است. اما پیاده‌سازی نرم‌افزاری با محدودیتهای کمتری مواجه بوده و با در اختیـار داشـتن کارتهای هوشمند و ابزارهای نرم‌افزاری و سخت‌افزاری مورد نیاز امکان‌پذیر خواهـد بـود. در حـال حاضـر در داخل کشور کارخانه تولید تراشه های الکترونیکی وجود نداشته و پس از طی مراحل طراحـی تراشـه بایـد ادامه فرآیند تولید تراشه در خارج از کشور دنبال گردد که این موضوع با محدودیتهای قانونی مواجـه اسـت. زیرا در پیاده‌سازی یک الگوریتم رمـز بـومی بـرای کاربردهـای خـاص انتشـار مشخصـات الگـوریتم رمـز بـا محدودیتهای قانونی مواجه بوده و بایـد کـل فراینـد پیـاده‌سـازی در داخـل کشـور انجـام گـردد. از ایـن رو پیاده‌سازی نرم‌افزاری الگوریتم رمز بومی بعنوان موضوع این پژوهش انتخاب گردیده است.

## ۱-۴. جنبه جدید بودن و نوآوری

در حال حاضر صرفاً الگوریتم‌های رمزنگاری اسـتاندارد بصـورت سـخت‌افـزاری و بـر روی بعضـی از کارتهای هوشمند در دسترس می‌باشد که بنا بر دلائل ارائه شـده در قسـمت قبـل در همـه کاربردهـا قابـل استفاده نمی‌باشند. در این پژوهش یک الگوریتم رمز بومی بصورت نرم‌افزاری بـر روی یـک کـارت هوشـمند پیاده‌سازی شده و شرایط لازم برای دستیابی به مناسب‌ترین حالت پیـاده‌سـازی از جهـت عملکـرد منطقـی، سرعت اجرا و امنیت برنامه‌نویسی بررسی خواهد شد.

## ۱-۵. 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).

## ۱-۶. ساختار پایان نامه

فصل اول : مقدمه و کلیات

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

---

[۵] IC

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 سخت‌افزار و نرم‌افزار کارتهای هوشمند مرور می‌گردد.

فصل چهارم : ساختار الگوریتم رمز بومی مورد نظر برای پیاده‌سازی بررسی و مشخصات آن بیان می‌گردد.

فصل پنجم : پیاده‌سازی نرم‌افزاری الگوریتم رمز بومی و روشهای بهینه نمودن آن ارائه خواهد شد.

فصل ششم : پیاده‌سازی نرم‌افزاری الگوریتم رمز بومی ارزیابی و با چند نمونه پیاده‌سازی قبلی مقایسه می‌گردد.

فصل آخر: به نتیجه‌گیری و جمع بندی موضوعات ارائه شده در فصول قبل پرداخته و موضوع پیشنهادی برای پژوهش‌های بعدی طرح خواهد شد.

## ۱-۷. خلاصه فصل

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