عنوان مقاله:

طراحی و پیاده سازی نرم افزاری مناسب یک الگوریتم رمز نگاری بلوکی بومی بر روی کارت هوشمند

محل انتشار:

فصلنامه مطالعات علوم کاربردی در مهندسی, دوره 10, شماره 1 (سال: 1403)

تعداد صفحات اصل مقاله: 13

نویسنده:

عبدالوهاب کمالی – مهندسی تکنولوزی نرم افزار

خلاصه مقاله:

امروزه سامانه های مبتنی بر کارت هوشمند به طور گسترده در سراسر دنیا رایج گردیده اند. کارت های هوشمند در کاربردهایی از قبیل کنترل دسترسی، تجارت الکترونیک، احراز هویت و از این قبیل استفاده می گردند. به خاطر اهمیت این کاربردها، ملاحظات امنیتی برای تولید کنندگان و کاربران کارت هوشمند حیاتی است. استفاده کنندگان وقتی می توانند 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 سخت افزاری و نرم افزاری 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 می گیرد. الگوریتمهای رمز با روشهای سخت افزاری یا نرم افزاری پیاده سازی و قابل بکارگیری می باشند. در این پایان نامه الگوریتم رمز aes با ساختار تغییر یافته، بعنوان الگوریتم رمز بومی در نظر گرفته شده و بصورت نرم افزاری بر روی کارت هوشمند top-imgx۴ ساخت شرکت gemalto پیاده سازی و با پیاده سازی های نرم افزاری الگوریتم aes که بر روی میکروکنترلر atmega۱۶۳ و میکروکنترلر ۸۰۵۱ انجام شده است و همچنین پیاده سازی های سخت افزاری الگوریتم aes که بر روی تراشه fpga مدل xc۲s۵۱۵-۶ و کارت هوشمند top-imgx۴ انجام گردیده، مقایسه شده است. نتایج حاصله نشانگر آن است که پیاده سازی نرم افزاری الگوریتم رمز بومی برای همه کاربردهای غیر بلادرنگ مناسب بوده اما برای کاربردهای بلادرنگ صرفا با افزایش منابع پردازشی و حافظه کارت هوشمند قابل استفاده خواهد بود.

کلمات کلیدی:

طراحی، پیاده سازی، نرم افزار، الگوریتم، رمز نگاری، بلوکی بومی، کارت هوشمند