عنوان مقاله:
تحلیل و ارزیابی روشهای تولید امضای دیجیتال

محل انتشار:
کنفرانس ملی مهندسی نرم افزار (سال: 1388)

تعداد صفحات اصل مقاله: 8

نویسنده:
روح الله کریمی - *دانشگاه آزاد اسلامی واحد قزوین - دانشکده برق ، رایانه و فناوری اطلاعات*

خلاصه مقاله:
اینترنت و برنامه های کاربردی تحت شبکه به سرعت در حال رشد هستند از اینرو نیاز به محافظت و تامین امنیت چنین برنامه هایی نیز افزایش یافته است.الگوریتمهای رمزنگاری نقش اصلی را در امنیت اطلاعات سیستمها و تولید امضای دیجیتال بازی می کنند.امضای دیجیتال کاملا مبتنی بر الگوریتمهای رمزنگاری بوده و باعث به رسمیت شناسی اطلاعات الکترونیکی شده به طوریکه هویت پدیدآورنده سند و جامعیت اطلاعات آن، قابل بازبینی و کنترل میباشد.از طرف دیگر الگوریتمهای مختلف رمزنگاری مقدار قابل ملاحضه ای از منابع سیستم مثل زمان CPU حافظه و توان باطری را مصرف می کنند.در این مقاله کوشش می کنیم علاوه بر تعریف و دسته بندی الگوریتمهای رمزنگاری به منظور تولید امضای دیجیتال به ارزیابی تعدادی از رایج ترین الگوریتمهای رمزنگاری مانند AES (Rijndael), DES, 3DES, RC2 RC6 و Blowfish پرداخته و مقایسه ای بر روی این الگوریتمها با اعمال تنظیمات مختلف بر روی هر یک از آنها مانند اندازه های متفاوت بلوکهای داده ، نوعهای داده متفاوت ، مصرف توان باطری ، اندازه کلیدهای مختلف و نهایتا سرعت رمزگذاری و رمزگشایی ، انجام دهیم. نتایج شبیه سازی نیز برای اثبات کارایی هر یک از این الگوریتم ها ارائه شده است

کلمات کلیدی:
الگوریتمهای رمزنگاری، رمزنگاری متقارن و نامتقارن، کلید عمومی و خصوصی