عنوان مقاله:
بررسی روش های امنیتی نوین در امضاهای دیجیتال

محل انتشار:
اولین کنفرانس ملی اصول مهندسی برق و کامپیوتر (سال: 1396)

تعداد صفحات اصل مقاله: 6

نویسندگان:
نعیمه شیخ بختیاری - *اطلاعات، گرایش تجارت الکترونیک، موسسه آموزش عالی بهمنیار کرمان، ایران کرمان، ایران*

علی ناصر اسدی - *گروه کامپیوتر، دانشگاه شهید باهنر کرمان، کرمان، ایران کرمان، ایران*

خلاصه مقاله:
اینترنت و کاربردهای تحت شبکه در حال گسترش است و افرا د بسیار زیادی وقت خو د را د ر اینترنت صرف تباد ل اطلاعات و تراکنش های مالی می کنند. بنابراین نیاز به تامین حفاظت و امنیت اطلاعات در اینترنت نیز از اهمیت ویژه ای برخوردار است. چون اینترنت فضایی باز تلقی می شود امکان استفاده ی این اطلاعات توسط افراد سودجو بسیار زیاد است. امروزه به دلیل ساختار غیرفیزیکی انتقال داده ها باید هنگام کار با اسناد الکترونیکی از علامتی برای تشخیص اصل بودن و سندیت بخشیدن به محتوا استفاده کرد. یکی از این شیوه ها امضای دیجیتال است. امضای دیجیتال نوعی رمزنگاری نامتقارن است که بر پایه ی الگوریتم های رمزگذاری شده به وجود آمده است که باعث به رسمیت شناختن اطلاعات الکترونیکی می شود به طوری که هویت پدید آورنده سند و جامعیت اطلاعات آن، قابل بازبینی و کنترل است. در این مقاله مروری ضمن بررسی امضاء دیجیتال، به تحلیل روش های تولید امضای دیجیتال می پردازیم. سپس سعی به بررسی و معرفی روش های مختلف و نوین مورد استفاده در امضا دیجیتال و همچنین روش های مختلف افزایش امنیت در این نوع از امضاها از جمله ساختارهای جدید در امضا دیجیتال و همچنین الگوریتم ها و تکنیک های پیشرفته در سال های اخیر برای مقابله با خطرات حملات امنیتی خواهد شد، در انتها با توجه به مرور ادبیات انجام شده در این حیطه در سال های اخیر، پیشنهاداتی برای تحقیقات آینده ارایه خواهد شد.

کلمات کلیدی:
امنیت، امضا دیجیتال، الگوریتم ها، کلید عمومی، کلید خصوصی