عنوان مقاله:

شیوههای رمزنگاری در شبکه های کامپیوتری : اصول، تکنیک ها و کاربردها

محل انتشار:

بیست و سومین کنفرانس بین المللی فناوری اطلاعات، کامپیوتر و مخابرات (سال: 1403)

تعداد صفحات اصل مقاله: 8

نویسنده:

حسین کاظمی – کارشناسی ارشد فناوری اطلاعات

خلاصه مقاله:

رمزنگاری ، علم و هنر محافظت از اطلاعات از طریق تبد یل دادهها به فرمتی غیر قابل خواندن برای افراد غیرمجاز است . این فناوری به دودسته اصلی متقارن و نامتقارن تقسیم می شود. در رمزنگاری متقارن، یک کلید مشترک برای رمزنگاری و رمزگشایی استفاده می شود، درحالی که در رمزنگاری نامتقارن، دو کلید متفاوت (عمومی و خصوصی) به کار م ی روند. از کاربردهای مهم رمزنگاری می توان به تامین محرمانگی و تمامیت دادهها، تایید هویت کاربران، و جلوگیری از انکار انجام تراکنش ها اشاره کرد. پروتکل های معروف مانند SSL/TLS و IPSec برای امنیت ارتباطات اینترنتی و شبکه ها طراحی شده اند. چالش های مهم پیش روی رمزنگاری شامل مقابله با توان محاسباتی کامپیوترهای کوانتومی و مدیریت ایمن کلیدهای رمزنگاری است . در آینده، توسعه الگوریتم های مقاوم در برابر کوانتوم و پیشرفت در رمزنگاری هومومورفیک و چندجانبه ایمن اهمیت زیادی خواهد داشت . در این مقاله باتوجه به گستردگی مطالب در این حوزه تنها به بررسی و معرفی اجمالی شیوههای رمزنگاری پرداخته شده است و امید است بتواند سرلوحه علاقه مندان به این حوزه باشد.

کلمات کلیدی:

رمزنگاری ، رمزنگاری متقارن، رمزنگاری نامتقارن، توابع دگرگون ساز