عنوان مقاله:
مروری بر الگوریتم های رمزنگاری

محل انتشار:
اولین کنفرانس مهندسی و فن آوری (سال: 1399)

تعداد صفحات اصل مقاله: 12

نویسندگان:
فرشته آقابیگی - *گروه مهندسی کامپیوتر، دانشکده فنیومهندسی، واحد اراک، دانشگاه آزاد اسلامی، اراک،*

نفیسه اوسطی عراقی - *استادیارگروه مهندسی کامپیوتر، دانشکده فنیومهندسی، واحد اراک، دانشگاه آزاد اسلامی، اراک*

سارا نظری - *استادیارگروه مهندسی کامپیوتر، دانشکده فنیومهندسی، واحد اراک، دانشگاه آزاد اسلامی، اراک،*

خلاصه مقاله:
در رمزنگاری، داده ها از ساختاری با معنی به ظاهری بی معنی تبدیل می شوند تا امنیت اطلاعات حفظ گردد. الگوریتم هایی با کلید متقارن و کلید نامتقارن، تابع Hash و رمزنگاری کوانتومی به منظور به کارگیری در حوزه های امنیتی مطرح شده اند. با وجود تمام تلاش هایی که برای حفظ حریم خصوصی اشخاص و تامین امنیت اطلاعات صورت پذیرفته است ولی همچنان افراد سودجو به دنبال طرح ریزی به منظور حمله به اطلاعات می باشند. ازاین رو، در این مقاله مروری، چندین الگوریتم رمزنگاری و حمله های مطرح بر آنان اشاره شده است تا دید کلی از رمزنگاری برای مطالعه کننده فراهم آید.

کلمات کلیدی:
رمزنگاری، الگوریتمهای با کلید متقارن، الگوریتمهای با کلید نامتقارن، تابع Hash، رمزنگاری کوانتومی، حمله به الگوریتمها