عنوان مقاله:
بررسی الگوریتم های رمزنگاری مناسب برای اینترنت اشیاء

محل انتشار:
دومین کنفرانس بین المللی پژوهش های دانش بنیان در مهندسی کامپیوتر و فناوری اطلاعات (سال: 1396)

تعداد صفحات اصل مقاله: 10

نویسندگان:
محمدعلی ترکمانی - *گروه مهندسی کامپیوتر، دانشکده مهندسی، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج ، ایران - واحد پژوهش، کارخانجات مخابراتی ایران، شیراز، ایران*

ریحانه نوروزی - *گروه مهندسی کامپیوتر، دانشکده مهندسی، عضو باشگاه پژوهشگران و نخبگان جوان واحد نی ریز نی ریزایران*

هادی ناصری - *گروه مهندسی کامپیوتر، دانشکده مهندسی، عضو باشگاه پژوهشگران و نخبگان جوان واحد استهبان، استهبان ایران*

خلاصه مقاله:
اینترنت اشیاء رهیافتی است که میتواند موجب ارتقای کیفی سطح زندگی انسان ها گردد. امروزه اینترنت اشیاء در کاربردهای مختلف نظامی، صنعتی، تجاری و مصارف خانگی مورد استفاده قرار می گیرد. استفاده از پتانسیل های اینترنت اشیاء، با چالش های مربوط به امنیت و حریم خصوصی روبرو است. در یک سامانه امن اینترنت اشیاء، نیازمندیهای مختلفی وجود دارد که مهمترین آنها عبارتند از محرمانگی، تایید هویت و صحت اطلاعات. با توجه به قدرت پردازشی کم، کمبود انرژی و محدودیت توان مصرفی گره های انتهایی اینترنت اشیاء و همچنین کمبود حافظه برای بار کردن نرم افزار، نیاز به الگوریتم های رمزنگاری سبک و امن می باشد تا بتوان از طریق آنها نیازمندی های امنیتی اینترنت اشیاء را تامین کرد. در این پژوهش تعدادی از الگوریتم رمزنگاری متقارن، نامتقارن و توابع درهم ساز از جنبه های مختلف نظیر امنیت، کارایی، طول کلید و مقاومت در برابر حملات مورد بررسی قرار گرفته و الگوریتم های مناسب برای اینترنت اشیاء معرفی می گردد. الگوریتم های متقارن، نامتقارن و توابع درهم ساز ذکر شده در این پژوهش، هم سبک بوده و هم بسیار امن می باشند و می توانند نیازمندی های امنیتی اینترنت اشیاء را برآورده سازند

کلمات کلیدی:
اینترنت اشیاء، رمزنگاری با کلید عمومی، رمزنگاری با کلید متقارن، تابع درهم ساز