عنوان مقاله:
ارائه الگوریتم رمزنگاری سبک برای دستگاههای اینترنت اشیاء با استفاده ازDNA

محل انتشار:
چهارمین کنفرانس ملی پدافند سایبری (سال: 1402)

تعداد صفحات اصل مقاله: 18

نویسندگان:
افشین برقیان - *دانشجوی کارشناسی ارشد مهندسی کامپیوتر، نرمافزار، دانشگاه آزاد واحد تهران شمال*

سحر صابری - *استادیار دانشگاه آزاد واحد تهران شرق*

زهره مافی - *عضو هیئت علمی، پژوهشگاه ارتباطات و فناوری اطلاعات*

خلاصه مقاله:
دستگاه های اینترنت اشیا نقشی اساسی در آسانتر، هوشمندانه تر و مجلل تر کردن زندگی انسانها دارند. این دستگاه ها اطلاعات مهمی از جمله اطلاعات شخصی، دادههای مهم و موارد دیگر را جمع آوری میکنند. با این وجود، دستگاه های اینترنت اشیا منابع محدودی دارند و به رمزگذاری تخصصی نیاز دارند که عملیات سبکی به نام رمزنگاری سبک را برای دستگاه های اینترنت اشیا و تضمین امنیت و حفاظت از آن دادهها انجام دهد. هدف این پژوهش پیشنهاد یک رمزنگاری سبک بر اساس نوار DNA به عنوان کلید با برخی عملیات برای تولید کلید برای دوره ای چند رمزنگاری و تابع آشوب استفاده میکند. روش پیشنهادی مبتنی بر DNA و تابع آشوب در دو عملیات اصلی جایگزینی و جابه جایی انجام میشود. روش پیشنهادی با استفاده از تصاویر مختلف پیاده سازی و آزمایش میشود و سپس برخی روشها مانند استاندارد رمزگذاری پیشرفته و استاندارد رمزگذاری سه گانه دادهه ا براساس معیارهای مختلف با آن مقایسه میشوند. علاوه بر این، راندمان دورهای رمزگذاری چندگانه روش پیشنهادی بهترین نسبت اعوجاج را هنگام استفاده از چهار دور به دست آورد. از سوی دیگر، کارایی استفاده از اندازه بلوک متغیر در روش پیشنهادی بهترین نتایج را برای زمانهای رمزگذاری و آنتروپی هنگام استفاده از اندازه بلوک ۱۲۸ بیتی به دست آورده است در حالی که بهترین نتایج از نسبت اعوجاج هنگام استفاده از ۷۲ بیت است. همه این نتایج تایید میکنند که روش پیشنهادی مبتنی بر DNA و تابع آشوب موثر است و میتواند برای مطابقت با منابع دستگاه های اینترنت اشیاء و اهمیت دادههای جمع آوری شده تغییر یابد.

کلمات کلیدی:
اینترنت اشیاء، رمزگذاری سبک، الگوریتم DNA، تابع آشوب، امنیت.