عنوان مقاله:

شبیه سازی و پیاده سازی یک رمز جریانی خودهمزمان بومی (CPS۳) جهت تامین امنیت داده ها در شبکه های الکترونیکی کشور

محل انتشار:

مجله پدافند غیر عامل, دوره 2, شماره 3 (سال: 1390)

تعداد صفحات اصل مقاله: 7

نویسندگان:

محمود یزدان پناه - *تهران اتوبان بابایی شهرک شهید رجایی بلوک ۵۸ واح ۶*

بهروز خادم

خلاصه مقاله:

تامین امنیت اطلاعات و حصول اطمینان از عدم دسترسی های غیر مجاز به اطلاعات سری در کشور و پایداری و خلل ناپذیری در فعالیت شبکه های الکترونیکی مدیریت و کنترل کشور (در سطح ملی و بخشی)، از جمله مهم ترین اهداف کلان پدافند غیرعامل در حوزه IT هستند. یکی از مهمترین ابزار مورد استفاده برای رسیدن به این اهداف، دانش رمزنگاری و کاربرد آن در طراحی شبکه های الکترونیکی امن کشور می باشد. از آنجا که رمز های جریانی، قابلیت های فراوانی در کاربردهای رمزنگاری برخط و با حجم داده بسیار زیاد دارند و نیز به طور گسترده در شبکه های الکترونیکی استفاده می شوند، لذا لازم است تحقیقات زیادی در زمینه طراحی و پیاده سازی آن ها انجام شود. در این مقاله، شبیه سازی و پیاده سازی یک رمز جریانی خودهمزمان آشوبی کلمه محور به نام CPS۳ روی یک نوع پردازنده ۸ بیتی خاص به نام ATMEGA۱۲۸ مورد مطالعه و بررسی قرار گرفته و با رمزهای منتخب در پروژه eSTREAM از نظر حجم حافظه مصرفی و سرعت تولید دنباله کلید مقایسه می شود.

کلمات کلیدی:

رمزجریانی, خودهمزمان, رمز آشوبی