عنوان مقاله:
ارزیابی کارایی الگوریتم های رمزنگاری متقارن

محل انتشار:
فصلنامه علوم و فنون دریایی, دوره 19, شماره 1 (سال: 1399)

تعداد صفحات اصل مقاله: 11

نویسندگان:
معصومه بیت عبدالله - *Faculty of Marine Engineering, Khorramshahr University of Marine Science and Technology, Iran*

محمد اسماعیل دوست - *Faculty of Marine Engineering, Khorramshahr University of Marine Science and Technology, Iran*

عامر کعبی - *Faculty of Marine Engineering, Khorramshahr University of Marine Science and Technology, Iran*

خلاصه مقاله:
با گسترش فناوری، نیاز به امنیت داده ها و اطلاعات بر روی بستر مخابراتی ضروری می باشد. یکی از موارد پراهمیت جهت برقراری امنیت اطلاعات، محیط های دریایی شامل ارتباطات مابین کشتی ها و همچنین ارتباط کشتی ها با ایستگاه های زمینی می باشد. جهت حفظ محرمانگی اطلاعات، الگوریتم های رمزنگاری متقارن مانند RC۶، IDEA، ۳DES، DES، Serpent و AES ارائه شده اند. گزارشات مختلفی توسط محققان جهت مقایسه کارایی این الگوریتم ها ارائه شده است. علی رغم بررسی های متنوع انجام شده، همچنان فقدان گزارشی جامع که از تمامی مناظر این الگوریتم ها را مورد مقایسه قرار دهد، احساس می شود. در این مقاله مقایسه و بررسی جامعی از منظر معماری، انعطاف پذیری، امنیت و سرعت اجرا انجام گرفته است تا براساس آن با توجه به کاربرد بتوان بر اساس انعطاف پذیری، سطح امنیت مورد نظر و یا سرعت اجرا نسبت به انتخاب الگوریتم اقدام نمود. نتایج پیاده سازی و مقایسات نشان دهنده برتری الگوریتم رمزنگاری AES در امنیت و RC۶ در سرعت اجرا می باشد.

کلمات کلیدی:
Cryptography, communication, Security, Symmetric key cryptography, Marine Communication