عنوان مقاله:
پیاده سازی کار آمد الگوریتم رمزنگاری Multi - prime RSA با استفاده از ضرب مونتگومری

محل انتشار:
کنفرانس ملی صنعت،تجارت و علوم دریایی (سال: 1398)

تعداد صفحات اصل مقاله: 8

نویسندگان:
محمد اسماعیل دوست - *استادیار دانشکده مهندسی دریا، دانشگاه علوم و فنون دریایی خرمشهر*

وحید زارعی - *مربی دانشکده مهندسی دریا، دانشگاه علوم و فنون دریایی خرمشهر*

خلاصه مقاله:
رمزنگاری RSA یکی از رایج ترین الگوریتم هایی است که در کاربرده های رمزنگاری، امضای دیجیتال و همچنین سیستم های امنیتی مورد استفاده قرار گرفته است. همگام با افزایش استفاده و محبوبیت این الگوریتم، تلاش های فراوانی برای بهبود سرعت عملکرد و همچنین بالا بردن سطح ایمنی این الگوریتم صورت پذیرفته است. Multi- prime RSA یکی از بهبود ها برروی رمزنگاری RSA می باشد که به منظور افزایش سرعت محاسبات، در آن از چند عدد اول به جای دو عدد اول در الگوریتم RSA استفاده شده است. در این مقاله ، برای دستیابی به عملکرد بهتر و افزایش سرعت محاسبات، فرایند رمزنگاری و رمزگشاییMulti - prime RSA با استفاده از ضرب مونتگومری انجام گردیده است. نتایج پیاده سازی، بهبود چشمگیری در سرعت اجرای الگوریتم Multi - prime RSA را نشان می دهد.

کلمات کلیدی:
رمزنگاری، کلید عمومی، RSA ضرب مونتگومری، Multi - prime RSA

لینک ثابت مقاله در پایگاه سیویلیکا: