عنوان مقاله:
بررسی معیار های مهم برای دستیابی به یک روش امن جهت ارسال کلید در الگوریتم های متقارن و نامتقارن در شبکه

محل انتشار:
هفتمین کنفرانس بین المللی دانش و فناوری مهندسی برق مکانیک و کامپیوتر ایران (سال: 1400)

تعداد صفحات اصل مقاله: 13

نویسندگان:
مرضیه معینی - *مدرس دپارتمان مهندسی برق و کامپیوتر، دانشگاه حضرت فاطمه، دانشگاه فنی حرفه ای استان کرمان، ایران*

هانیه شجاعی - *دانشجوی کاردانی نرم افزار کامپیوتر دانشگاه الزهرا*

حانیه محمدی - *دانشجوی کاردانی نرم افزار کامپیوتر دانشگاه الزهرا*

مهلا سلطانی نژاد - *دانشجوی کاردانی نرم افزار کامپیوتر دانشگاه الزهرا*

خلاصه مقاله:
سیستم های رمزنگاری در حال حاضر به دو دسته عمده رمزنگاری متقارن (Symmetric Cryptography) و رمزنگاری نامتقارن (Asymmetric Cryptography) تقسیم می شوند. در حالی که رمزگذاری متقارن اغلب به عنوان مترادفی برای رمزنگاری متقارن استفاده می شود رمزنگاری نامتقارن شامل دو مورد کاربردی اصلی یعنی رمزگذاری نامتقارن و امضای دیجیتال است. با توجه به پیشرفت روز افزون تکنولوژی وجود الگوریتم های رمزنگاری برای افزایش سطح ایمنی یک ضرورت به حساب می آید. در این مقاله سعی کرده ایم تا با بررسی معیار های مهم برای پیدا کردن امن ترین روش برای ارسال کلید در الگوریتم های متقارن در شبکه به این هدف دست یابیم که کدام روش مناسب تر و بهتر است. سعی کرده ایم تا با مقایسه عملکرد دو نوع از الگوریتم های متقارن و نامتقارن به این هدف برسیم که کدامیک موثرتر و ایمن تر هستند .

کلمات کلیدی:
الگوریتم های متقارن، الگوریتم های نامتقارن، کلید، امنیت اطلاعات، رمزنگاری