عنوان مقاله:
روش جدید برای رمزنگاری بر مبنای کلید متقارن، جایگزینی و جابجایی

محل انتشار:
همایش ملی ابتکار نوین و کاربردی در مهندسی برق و کامپیوتر با رویکرد دانش بنیان (سال: 1397)

تعداد صفحات اصل مقاله: 8

نویسندگان:
احمد یوسفی - *عضو هییت علمی گروه کامپیوتر، دانشگاه آزاد اسلامی، ایران، نایین*

مصطفی بنی طبا - *عضو هییت علمی گروه علوم پایه، دانشگاه آزاد اسلامی، ایران، نایین*

خلاصه مقاله:
هر گاه صحبتی از ارتباطات به میان می آید یکی از مباحث بسیار مهم در ارتباط برقراری امنیت آن است. با توجه به وجود عوامل مزاحم و نیروهای تهدیدکننده در محیط های تبادل پیام ها که به طور قابل توجهی در حال افزایش می باشند، حفظ محرمانگی و اعتبار پیام ها یکی از مقوله های بسیار بسیار مهم در تبادل پیام ها است. برای رسیدن به این هدف از رمزنگاری پیام ها استفاده می شود. در این مقاله، یک روش جدید ارایه خواهد شد که با استفاده از کلید متقارن، جایگزینی و جابجایی، بطور قابل توجهی ابهام و درهم ریختگی را در پیام ها بوجود خواهد آورد و یا به عبارتی دیگر، پیام ها را رمز خواهد کرد تا عوامل مزاحم و نیرو های تهدید کننده با بدست آوردن پیام ها از محیط تبادل آنها نتوانند پیام اصلی را بدست بیاورند.

کلمات کلیدی:
رمز نگاری، رمز گشایی، کلید متقارن، جایگزینی، جابجایی، تهدید کننده