

عنوان مقاله:

تحلیل و بهینه سازی سیستم رمز سزار تعمیم یافته

محل انتشار:

یازدهمین کنفرانس دانشجویی مهندسی برق (سال: 1387)

تعداد صفحات اصل مقاله: ۶ صفحه

نویسنده:

مجتبی سلطانهیان - دانشکده برق دانشگاه صنعتی شریف

خلاصه مقاله:

در این مقاله به بررسی رمز سزار تعمیم یافته پرداخته شده است. در این نوع رمز سزار الگوریتم رمزنگاری ممکن است بیش از یک بار روی رشته سمبرل ها اعمال شود. رویکرد کلی مقاله استفاده از دانش جایگشت ها برای بررسی این گونه رمزنگاری است. راهکارهایی برای اجرای دستی الگوریتم های مبتنی بر سیستم رمز سزار تعمیم یافته و همچنین برای بهینه سازی کلید آنها ارائه شده اند. در ادامه لم ها و قضایای مطرح شده راهگشای معرفی ابزاری فرکانسی روی چنین رمزنگاری بوده است.

کلمات کلیدی:

الگوریتم سزار، الگوی کدگذاری، حروف پایه و مبدل، خودرسی

لینک ثابت مقاله در پایگاه سیولیکا:

https://www.civilica.com/Paper-ISCEE11-ISCEE11_111.html

این صفحه به معنای تاییدیه نمایه سازی مقاله در پایگاه استنادی سیولیکا می باشد. در هر لحظه به منظور تایید اصالت این گواهی می توانید وضعیت ثبت مقاله را از طریق لینک فوق به صورت آنلاین کنترل نمایید.