

عنوان مقاله:

شکستن الگوریتم رمزنگاری ویجینر با استفاده از الگوریتم بهینه سازی اجتماع ذرات مشارکتی MPSO

محل انتشار:

دومین کنفرانس ملی مهندسی نرم افزار دانشگاه آزاد لاهیجان (سال: 1391)

تعداد صفحات اصل مقاله: 5

نویسندگان:

بابک اسدی - دانشگاه آزاد اسلامی واحد اراک

مهدی احمدی پری - دانشگاه آزاد اسلامی واحد اراک

خلاصه مقاله:

الگوریتم رمزنگاری ویجینر یکا لگوریتم متقارن است که با استفاده از یک کلید و جایگزینی حروف متن آن را رمزنگاری می کند در این مقاله ما قصد داریم روشی ارایه کنیم که فقط با در اختیار بودن متن رمز شده کلید رمز را پیدا کند در این روش ما از یک الگوریتم اجتماع ذرات بهبود یافته که با نام الگوریتم بهینه سازی اجتماع ذرات مشارکتی MPSO شناخته می شود استفاده می کنیم همچنین نشان میدهیم که MPSO از الگوریتم اجتماع ذرات استاندارد PSO بهتر عمل میکند.

کلمات کلیدی:

تحلیل رمز الگوریتم اجتماع پرندگان، الگوریتم اجتماع پرندگان مشارکتی ، الگوریتم رمز نگاری ویجینر، PSO, MPSO
cryptography

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/184814>

