

عنوان مقاله:

شکستن الگوریتم رمز نگاری ویجینر با استفاده از الگوریتم بهینه‌سازی گروه ذرات PSO

محل انتشار:

همایش منطقه ای علوم کامپیوتر، مهندسی کامپیوتر و فناوری اطلاعات (سال: 1391)

تعداد صفحات اصل مقاله: 8

نویسندگان:

مهدی احمدی پری - دانش کارشناسی ارشد - گروه کامپیوتر دانشگاه آزاد اسلامی واحد اراک

بابک اسدی - دکترای ریاضی - گروه ریاضی دانشگاه آزاد اسلامی واحد اراک

خلاصه مقاله:

شکستن الگوریتم های رمز نگاری به دلایل مختلف مورد توجه دانشمندان علم رمز نگاری قرار گرفته است . روش های مختلفی نیز برای این کار اقدام شده است. یکی از روش های جدید و شکستن الگوریتم ها رمز نگاری استفاده از هوش مصنوعی است. در این مقاله ما یکی از روش های هوش مصنوعی که حرکت دسته جمعی پرندگان و حرکت گله ماهی ها الهام گرفته شده و با نام الگوریتم به اجتماع ذرات شناخته می شود را برای رمز شکنی مورد * قرار می دهیم و کارایی آن را بر روی یکی از الگوریتم های رمز نگاری به نام ویجینر مورد آزمایش قرار می دهیم.

کلمات کلیدی:

تحلیل رمز، الگوریتم اجتماع پرندگان، الگوریتم رمز نگاری ویجینر ، PSO

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/173542>

