عنوان مقاله:
بررسی آسیب پذیری امنیت یک دستگاه رمزنگاری مبتنی بر توابع بازگشتی لوکاس، به کمک کسرهای مسلسل

محل انتشار:
دومین کنفرانس بین المللی مکانیک، برق، مهندسی هوافضا و علوم مهندسی (سال: 1401)

تعداد صفحات اصل مقاله: 9

نویسندگان:
شاهد مشهودی - *گروه ریاضی، دانشکده علوم پایه، دانشگاه آزاد اسلامی واحد رشت، ایران*

مهسا صادقی - *دانشکده علوم ریاضی و کامپیوتر، دانشگاه خوارزمی، تهران، ایران*

خلاصه مقاله:
مقاله حاضر به تعمیم الگوریتم شکستن رمز به وسیله ی کسرهای مسلسل، برای یک دستگاه رمزنگاری مبتنی بر توابع بازگشتی لوکاس می پردازد. در ابتدا پس از مروری بر بعضی تعاریف اولیه و پیش نیازها، به بررسی توابع بازگشتی لوکاس و ویژگی های جبری خاص آنها، می پردازیم تا به کمک آنها بتوانیم دستگاه رمز لوکاس و ارتباط آن با دستگاه های قبلی رمزنگاری را توضیح دهیم. سپس ضمن اشاره به کسرهای مسلسل و کاربرد آنها در تقریب های دیوفانتی، روش شکستن رمز به وسیله ی کسرهای مسلسل را به دستگاه رمز لوکاس تعمیم می دهیم. در خاتمه نشان می دهیم که موفقیت این روش به برقراری شرایط خاصی وابسته است که با رعایت استانداردهای لازم از ابتدا، می توان امنیت سیستم را تامین کرد.

کلمات کلیدی:
توابع بازگشتی لوکاس، دستگاه رمز لوکاس، کسرهای مسلسل، شکستن رمز