مقایسه الگوریتم های ریاضی و کلیدهای رمزنگاری با رویکرد انتظامی

سمیه حدادی[1] ، دکتر طاهر لطفی[2]

چکیده

در این پژوهش با روش تحقیق مقایسه ای (قیاسی) فرض کردیم a و b دو عدد مثبت باشند به طوری که $a>b$ باشد. در روش الگوریتم اقلیدسی برای یافتن بزرگترین عامل مشترک بین دو عدد a و b که با نماد $gcd(a,b)$ و یا به طور خلاصه به صورت (a,b) نمایش می دهند. الگوریتم را به این صورت بیان کردیم : ابتدا انتخاب می کنیم $r_0=a$ و $r_1=b$ داریم.

با اثبات قضیه های مختلف و در تحقیق انجام شده و بررسی و مقایسه الگوریتم های رمزنگاری، الگوریتم اقلیدسی و قضیه چینی و قضیه لاگرانژ مشخص شد الگوریتم اقلیدسی روش مناسب رمزنگاری اطلاعات برای مراکز نظامی و انتظامی می باشد. نتایج این تحقیق می تواند در طراحی الگوریتم های کدگذاری اطلاعات و داده های محرمانه و اسناد انتظامی کاربرد داشته باشد.

واژگان کلیدی: *الگوریتم رمزنگاری، کلید ریاضی، امنیت انتظامی داده ها*

[1] دانشجوی کارشناسی ارشد ریاضی کاربردی، دانشگاه آزاد اسلامی، واحد همدان somayeh.hadadi@gmail.com
[2] استادیار گروه ریاضی دانشگاه آزاد اسلامی، واحد همدان