نشریه علمی-تخصصی
پژوهش های نوین علوم مهندسی
ISSN: 2538-3809
سال پنجم، شماره ۳ (پیاپی: ۳۱)، پاییز ۱۳۹۹

الگوریتم هش MD-Caspian (بهینه شده MD5)

تورج استواری[۱]

تاریخ دریافت: ۹۹/۰۶/۲۳
تاریخ پذیرش: ۹۹/۰۷/۳۰
کد مقاله: ۹۹۸۰۱

چکـیده

در این مقاله سعی شده با روش‌های ساده و گیت N A N D یک تابع یک‌طرفه که امن و مشکلاتی همچون تصادم (Collision) که در MD5 مشاهده شده بود رفع گردد. همچنین از الگوریتم B E L که نوعی P R N G اما مناسب اعمال رمزنگاریست استفاده شده و میشود گفت C S P R N G هم تلقی میگردد استفاده گردیده و اعمال بیتی همراه گیت های X O R, , N A N D صورت پذیرفته. از عیوبی که این الگوریتم دارد می‌توان به سرعت نسبتا کمتر آن نسبت بهMD5 است. در متن مقاله شبه کد نوشته شده جهت پیاده سازی نرم افزاری و کارآمدبودن فهم متن مقاله استفاده شده است.

واژگـان کلـیدی: MD5,One Way Functions, Hash

۱- کارشناسی مهندسی نرم افزار دانشگاه فنی و حرفه ای شماره یک، تبریز، ایران، *Toraj.ostovari@gmail.com*