این نوع از الگوریتم های Hash توسط آقای رونالد ری وست معرفی گردید .در واقع این تابع درهم ساز نسخه پنجم از توابعی است که آقای ری وست برای محاسبه چکیده پیام در سال ۱۹۹۱ ارائه کرد .

این الگوریتم ها در ۱۵ سال اخیر کاربردهای بسیاری پیدا کرده است ولی این تابع درهم ساز نیز مانند اسلاف پیشین خود (MD4,MD3,……) در ۱۸ مارس سال ۲۰۰۶ توسط یک کامپیوتر کیفی در عرض یک دقیقه جعل شد و پیام مشابه ای تولید گردید .

الگوریتم MD5 پیامی را با هر طولی پذیرفته و آن را به قطعات ۵۱۲ بیتی تقسیم می کند ، با این استثنا که اخرین قطعه باید ۴۴۸ بیت باشد تا با احتساب ۶۴ بیت که به انتهای آن اضافه می شود تا کلیه قطعات به صورت ۵۱۲ بایتی درآیند .

هرگاه طول مناسب نباشد به انتهای آن مقادیر زائد اضافه می شود .هر بلوک ۵۱۲ بایتی در آرایه ای ذخیره می شود و داده های این آرایه درهم سازی می شوند و سپس مقادیر با هم جمع شده و شیفت داده می شوند . در این روش طول چکیده پیام ۱۶ بایت است .

الگوریتم MD5 درسطح بسیار وسیعی برای تضمین دست نخوردگی و سلامت داده ها کاربرد یافته بود و نهایتا در سال ۲۰۰۶ شکست خورد و در واقع یک برخورد (collision)کشف گردید .