الگوریتم HMAC

در Hashing در هنگام ارسال بسته مهاجم می تواند روی بسته تغییرات مورد نظر خود را ایجاد و سپس اقدام به تولید hash برای این دیتا بکند و سپس این hash را جایگزین hash اصلی کند به این ترتیب در مقصد hash تولید شده توسط گیرنده برای دیتا با hash ارسالی یکسان خواهد بود و متوجه تغییر بسته نخواهند شد.

برای جلوگیری از این مشکل از مکانیزم (Hashed Message Authentication Code HMAC) استفاده می شود. که در آن برای تولید hash علاوه بر دیتا بسته از یک secret key نیز استفاده می شود. این secret key را فقط دو طرف ارتباط دارند در نتیجه مهاجم این secret key را ندارد و اگر بین راه مهاجم تغییر روی بسته ایجاد کند و برای آن یک hash تولید کند مطمئنا در مقصد نتیجه hash ها یکسان نخواهد بود چون مهاجم secret key را برای تولید Hash ندارد.

در رمزنگاری، کد اصالت‌سنجی پیام برپایه درهم‌سازی (HMAC)، ساختار معینی برای محاسبه کد تأیید هویت پیام (MAC) است که شامل یک تابع درهم ساز رمزنگاری در ترکیب با یک کلید رمز است. HMAC نیز مانند هر MAC، می‌تواند جامعیت داده و اعتبار یک پیام را همزمان بررسی کند. هر تابع درهم ساز رمزنگاری مانند MD5 یا SHA-1، را می‌توان برای محاسبهٔ HMAC استفاده کرد. به این ترتیب الگوریتم MAC نتیجه شده، HMAC-MD5 یا HMAC-SHA1 نامیده می‌شود. قدرت رمزنگاری HMAC به قدرت رمزنگاری تابع درهم ساز به کاررفته در آن، اندازهٔ بیتی طول خروجی درهم ساز آن و اندازه و کیفیت کلید رمزنگاری بستگی دارد.  
یک تابع درهم ساز تکراری، پیام را به بلوک‌هایی با اندازه معین تقسیم می‌کند و تابع فشرده‌سازی را روی آنها تکرار می‌کند. به عنوان مثال، MD5 و SHA-1، روی بلوک‌های 512 بیتی عمل می‌کنند. اندازهٔ خروجی HMAC با انداره تابع درهم ساز به کاررفته در آن یکسان است. (در حالت MD5یا SHA-1، 128 یا 160 بیت). هرچند این اندازه می‌تواند در صورت لزوم کوتاه شود.



