Hیک تابع درهم‌ساز رمزنگاری است.

K کلید رمزی است که تعدادی صفر به سمت راست آن اضافه شده‌است تا اندازه بلوک‌های تابع درهم‌ساز شود.

m پیامی است که باید تأیید هویت شود.

|| نشاندهنده عمل الحاق است.

⊕ نشاندهنده یای انحصاری است (XOR)

opad اضافه کردن بیت خارجی است (0x5c5c5c…5c5c، ثابت هگزادسیمال به اندازه طول یک بلوک)

ipad اضافه کردن بیت داخلی است (0x363636…3636، ثابت هگزادسیمال به اندازه طول یک بلوک)

بنابراین تعریف ریاضی (HMAC(K,m به صورت زیر است:

HMAC (K,m) = H((K ⊕ opad) ∥ H((K ⊕ ipad) ∥ m))

اصول طراحی

انگیزه طراحی خصوصیات HMAC بدلیل وجود حمله‌ها به مکانیسم‌های بی‌اهمیت بیشتری ایجاد شد تا یک کلید را با یک تابع درهم ساز ترکیب کند. به عنوان مثال، یک نفر ممکن است فرض کند امنیتی که HMAC فراهم می‌کند، همان امنیتی است که می‌توان با ‎ MAC = H(key ∥ message)‎ بدست آورد. درحالیکه این روش دارای نقص‌های جدی است: در اکثر توابع درهمساز، بدون دانستن کلید، می‌توان به راحتی داده‌هایی را به پیام اضافه نمود و MAC معتبر دیگری بدست آورد. همچنین، اضافه کردن کلید با استفاده از‎ MAC = H(message ∥ key)‎ دارای این مشکل است که مهاجمی که بتواند در تابع درهم ساز (بدون کلید) برخوردی پیدا کند، در MAC هم می‌تواند پیدا کند. با اینکه مقاله‌های امنیتی متعددی به آسیب پذیری‌هایی در‎ MAC = H(key ∥ message ∥ key)‎، حتی زمانیکه از دو کلید متفاوت استفاده می‌شود، اشاره داشته‌اند، اما استفاده از این رویکرد بهتر است.

هیچ حمله پسوندی شناخته شده‌ای دربرابر خصوصیات HMAC فعلی که به صورت‎ H(key1 ∥ H(key2 ∥ message))‎ تعریف شده، یافت نشده‌است. زیرا درخواست تابع درهمساز بیرونی، نتیجه متوسط درهم ساز داخلی را پنهان می‌کند. مقادیر ipad و opad، برای امنیت این الگوریتم، قطعی نیستند. اما برای داشتن فاصله همینگ بزرگ از یکدیگر تعریف شده‌اند. به این ترتیب کلیدهای داخلی و خارجی، بیت‌های مشترک کمتری خواهند داشت.

امنیت

قدرت رمزنگاری HMAC بستگی به اندازه کلید رمز مورد استفاده دارد. شایع‌ترین حمله روی HMACها برای کشف کلید رمز، حمله کورکورانه‌است. HMACها به‌طور قابل ملاحظه‌ای کمتر از الگوریتم‌های درهمساز به کاررفته در آن‌ها تحت تأثیر برخوردها قرار می‌گیرند.

در سال ۲۰۰۶، جانگ سونگ کیم، الکس بیریوکف، بارت پرنیل و سوکی هونگ نشان دادند چگونه می‌توان HMAC با نسخه‌های کاهش یافته MD5 یا SHA-1 یا نسخه‌های کامل HAVAL، MD4 و SHA-0 را از یک تابع تصادفی یا HMAC با یک تابع تصادفی تشخیص داد. تمایزدهنده‌های تفاضلی به مهاجم این اجازه را می‌دهند که یک حمله ساختگی روی HMAC ترتیب دهد. علاوه بر این، تمایزدهنده‌های مستطیلی و تفاضلی می‌توانند منجر به حمله‌های پیش‌تصویر دوم شوند. HMACی که از نسخه کامل MD4 استفاده می‌کند، می‌تواند با این آگاهی‌ها جعل شود. این حمله‌ها تناقضی برای اثبات امنیت HMAC نیست بلکه بینشی از HMAC را براساس توابع درهم ساز رمزنگاری موجود ارائه می‌دهد.

