برای درک نحوه کار HMAC ، ابتدا بررسی کنیم که چگونه می توان از یک تابع هش (به تنهایی) برای انجام بررسی یکپارچگی داده ها در انتقال پرونده استفاده کرد. بیایید بگوییم یک برنامه مشتری یک فایل را از یک سرور از راه دور بارگیری می کند. فرض بر این است که سرویس گیرنده و سرور قبلاً درباره یک عملکرد هش مشترک توافق کرده اند ، مثلا SHA2.

قبل از اینکه سرور پرونده را ارسال کند ، ابتدا یک هش از آن فایل را با استفاده از عملکرد هش SHA2 بدست می آورد. سپس آن هش (هضم پیام a.k.a) را به همراه خود فایل ارسال می کند. مشتری با دریافت دو مورد (یعنی فایل بارگیری شده و هش) ، SHA2 هش فایل بارگیری شده را بدست می آورد و سپس آن را با هش بارگیری شده مقایسه می کند. اگر این دو مورد با هم مطابقت داشته باشند ، این بدان معناست که پرونده در طول مسیر دستکاری نشده است.

اگر یک مهاجم موفق شود فایل بارگیری شده را رهگیری کند ، محتوای فایل را تغییر دهید و سپس پرونده دستکاری شده را به گیرنده هدایت کنید ، این عمل مخرب بدون توجه نخواهد بود. این به این دلیل است که ، هنگامی که مشتری پرونده دستکاری شده را از طریق الگوریتم هش توافق شده اجرا می کند ، هش حاصل شده با هش بارگیری شده مطابقت ندارد. با این کار گیرنده می فهمد که پرونده در طول مسیر خود دستکاری شده است.

بنابراین یک تابع هش باید کلاهبرداری کند؟ نه خیلی سریع. در حالی که یک تابع هش می تواند یکپارچگی داده ها را ایجاد کند ، به عنوان مثال فایل یا پیام در طول مسیر تغییر نکرده است ، اما نمی تواند صحت را ثابت کند. مشتری از کجا می داند پیامی را که از منبع قانونی دریافت کرده است؟

به همین دلیل پروتکل های انتقال فایل امن مانند FTPS ، SFTP و HTTPS از HMAC به جای فقط توابع هش استفاده می کنند. هنگامی که دو طرف پیام را از طریق آن پروتکل های امن انتقال فایل رد و بدل می کنند ، این پیام ها به جای هش های ساده با HMAC همراه می شوند. HMAC هم از تابع هش و هم از یک کلید مخفی مشترک استفاده می کند.

یک کلید مخفی مشترک راهی برای تبادل احزاب برای تأیید صحت پیام فراهم می کند. یعنی دو طرف راهی را برای تأیید اینکه آیا پیام و MAC (به طور خاص HMAC) دریافت می کنند واقعاً از حزبی است که قرار است با آنها معامله کنند ، فراهم می کند.

کلید مخفی این قابلیت را امکان پذیر می کند زیرا در حین تبادل کلید تولید می شود ، یک فرآیند اولیه که به مشارکت دو طرف نیاز دارد. فقط آن دو طرفی که در تبادل کلید شرکت کرده اند می دانند کلید مخفی مشترک چیست. در عوض ، آنها تنها کسانی هستند که در صورت محاسبه MAC مربوط به پیام با استفاده از کلید مخفی مشترک ، می توانند به همان نتیجه برسند.