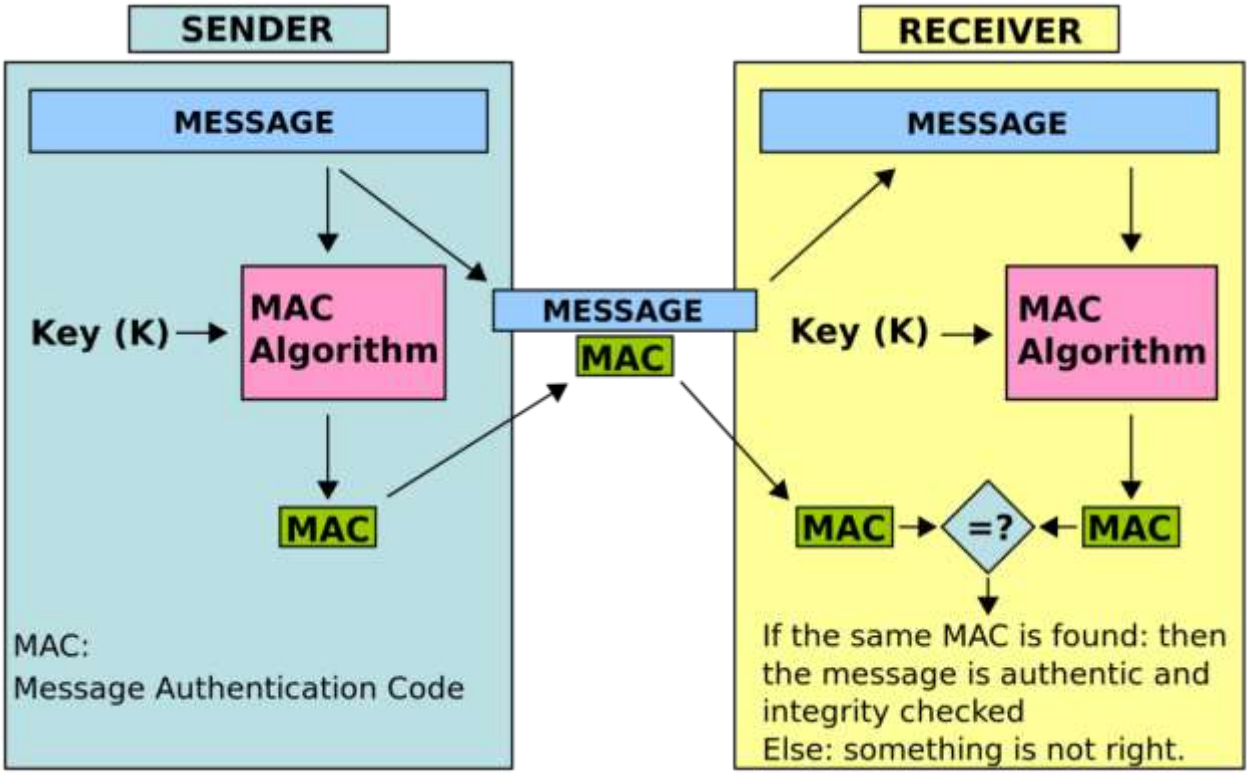
الگوریتم HMAC

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 hashاصلی 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 keyرا 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 .
HMACنیز مانند هر MAC، می‌تواند جامعیت داده و اعتبار یک پیام را همزمان بررسی کند. هر تابع درهم ساز رمزنگاری مانند MD5 یاSHA-1 ، را می‌توان برای محاسبهٔ HMAC استفاده کرد. به این ترتیب الگوریتم MACنتیجه شده، HMAC-MD5یا 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، MD5وSHA-1 ، روی بلوک‌های ۵۱۲ بیتی عمل می‌کنند. اندازهٔ خروجی HMAC با اندازه تابع درهم ساز به کاررفته در آن یکسان است.در حالتMD5 یاSHA-1 ، ۱۲۸ یا ۱۶۰ بیت .(هرچند این اندازه می‌تواند در صورت لزوم کوتاه شود).


SENDER
RECEIVER
MESSAGE
MESSAGE
Key (K)
MAC Algorithm
MESSAGE
MAC
Key (K)
MAC Algorithm
MAC
MAC
=?
MAC
MAC:
Message Authentication Code
If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.


CrypTool 2.1 (Stable Build 8853.3) – HMAC.cwm
Classic Ciphers
ADFGVX
Caesar
Enigma
Fialka
Hill Cipher
Modern Ciphers
Steganography
Hash Functions
Cryptanalysis
Protocols
Tools