MD5 (Message Digest Algorithm 5) versus (Secured Hash Algorithm-1) SHA-1 versus DES versus 3DES versus AES versus blah blah blah

Setting up an IPsec connection involves all kinds of crypto choices, but this is simplified substantially by the fact that any given connection can use at most two or (rarely) three at a time.

Authentication calculates an Integrity Check Value (ICV) over the packet's contents, and it's usually built on top of a cryptographic hash such as MD5 or SHA-1. It incorporates a secret key known to both ends, and this allows the recipient to compute the ICV in the same way. If the recipient gets the same value, the sender has effectively authenticated itself (relying on the property that cryptographic hashes can't practically be reversed). AH always provides authentication, and ESP does so optionally.

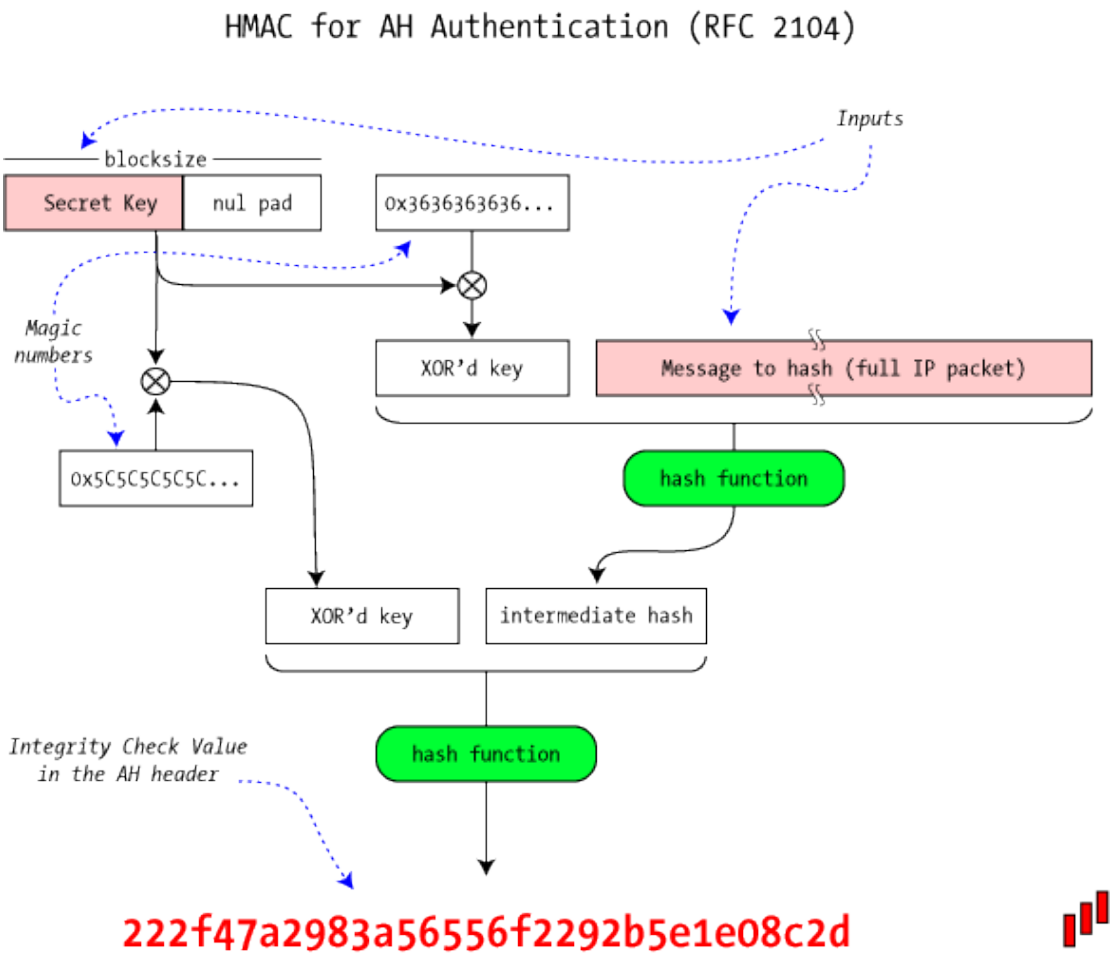
Encryption uses a secret key to encrypt the data before transmission, and this hides the actual contents of the packet from eavesdroppers. There are quite a few choices for algorithms here, with DES, 3DES, Blowfish and AES being common. Others are possible too.

Authentication Algorithms

AH carries an Integrity Check Value in the Authentication Data portion of the header, and it's typically (but not always) built on top of standard cryptographic hash algorithms such as MD5 or SHA-1.

Rather than use a straight checksum, which would provide no real security against intentional tampering, it uses a Hashed Message Authentication Code (HMAC) which incorporates a secret value while creating the ICV. Though an attacker can easily recompute a hash, without the secret value he won't be able to recreate the proper ICV. HMAC is described by RFC 2104, and this illustration shows how the message data and secret contribute to the final

Integrity Check Value:



We'll note that IPsec/AH doesn't define what the authentication function must be, it instead provides a framework which allows any reasonable implementation *agreed to by both ends* to use. It's possible to use other authentication functions, such as a digital signature or an encryption function as long as both sides provide for it.