Anthony Constantino
HW 4

HMAC

From my understanding, Hashed MACs are created but making the hashing values dependent on some sort of symmetric encryption key. They are then used to hash the MAC and you are left with a HMAC. This is convenient because then a message can be sent and only if you have that exact symmetric key you can run it through the same algorithm to decrypt the message in the same way it was encrypted because the key is symmetric. The way it does this is by concatenating the secret to the front the message, hashes it, attaches the key to the front of it again and hashes it again, making it expensive.