**HMAC**

HMAC is the current industry standard as CBC-MAC is deemed to be slow

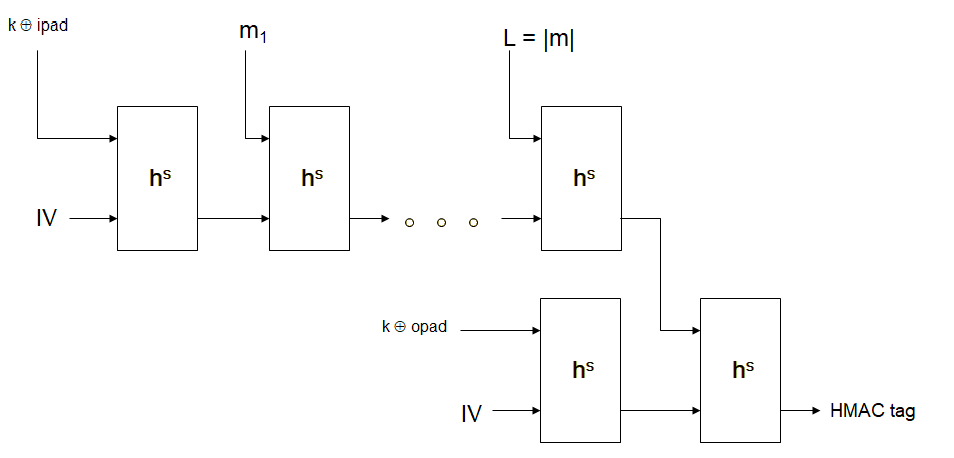
(Gen, h): A fixed length hash function

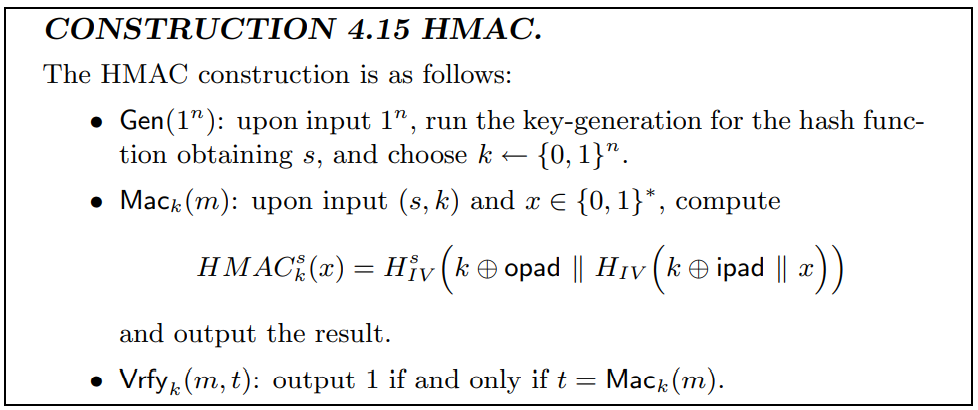
(Gen, H): Hash function after applying MD transform to (Gen, h)

Fixed constants: IV, opad (outer pad), ipad (inner pad)

Opad: 0x36 repeated as many times as needed

Ipad: 0x5C repeated as many times as needed





References

[1] J. K. a. Y. Lindell, Introduction to Modern Cryptography.

[2] B. Micali, "Hardcord bits," [Online]. Available: <https://crypto.stanford.edu/pbc/notes/crypto/hardcore.html>.

[3] Lecture Slides