2021201041
Nvss Maneesh Gupta

HMAC

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

(Gen, h): A fixed length hash function

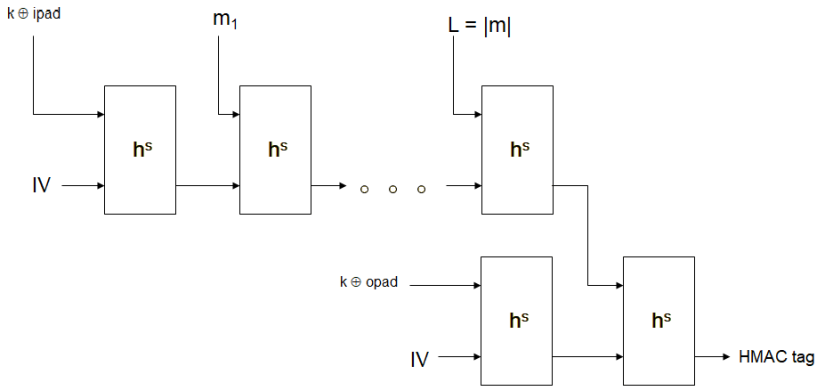
(Gen, H): Hash function after applying MD transform to (Gen, h)

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

$$HMAC\ tag\ for\ m = H^s_{IV}((k \oplus opad) \parallel H^s_{IV}((k \oplus ipad) \parallel m))$$



CONSTRUCTION 4.15 HMAC.

The HMAC construction is as follows:

- $\mathsf{Gen}(1^n)$: upon input 1^n, run the key-generation for the hash function obtaining s, and choose $k \leftarrow \{0,1\}^n$.
- $\mathsf{Mac}_k(m)$: upon input (s,k) and $x \in \{0,1\}^*$, compute

$$HMAC^s_k(x) = H^s_{IV}\Big(k \oplus \mathsf{opad} \parallel H_{IV}\Big(k \oplus \mathsf{ipad} \parallel x\Big)\Big)$$

  and output the result.
- $\mathsf{Vrfy}_k(m,t)$: output 1 if and only if $t = \mathsf{Mac}_k(m)$.

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