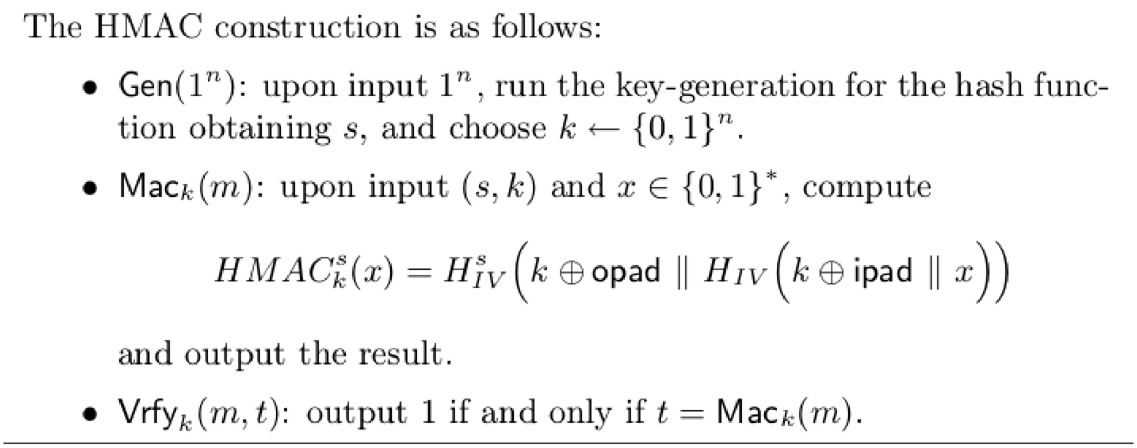
Hash based Message authentication code (HMAC):

It is a type of message authentication code which is based on hashing technique. Like MACs it is used for data integrity and authentication.

The construction of HMAC relies on the following two points

- The hash function constructed using Mekle-Damgard transform is collision resistant.
- The fixed-length collision resistant hash function has certain pseudo randomness or MAC-like properties.

Construction:



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

$$HMAC_k^s(x) = H_{IV}^s\Big(k \oplus \mathsf{opad} \parallel H_{IV}\Big(k \oplus \mathsf{ipad} \parallel x\Big)\Big)$$

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

In the HMAC construction we use two constants **opad** and **ipad** which are having length of n (block length). The string opad is formed by repeating the byte **36** in hexadecimal as many times as needed; the string ipad is formed in the same way using the byte **5C**.

We perform XOR between k and ipad and will concatenate it to x and then we will compute inner hash $H_{IV}^{s}(k\,XOR\,ipad \,\|\, x)$ and the outer hash is computed by $z' = h^s\,(IV \,\|\, k\,XOR\,opad)$ which implies $h^s\,(IV \,\|\, k\,XOR\,ipad)$ and $h^s\,(IV \,\|\, k\,XOR\,opad)$ are two different pseudorandom keys k_1, k_2 respectively.

$$HAMC_k^s(x) = H_{IV}^s\big(k\,XOR\,opad \,\|\, H(k\,XOR\,ipad \,\|\, x)\big) = H_{k_1}^s\left(H_{k_2}^s(x)\right)$$