(Gen, h): A fixed length hash function
(Gen, H): A gash function after applying Merkle-Demgard transform to (Gen, h).
Fixed constants: Initialisation vector, opad, ipad.
HMAC tag for m = $\mathbf{H^s_{IV}((k \oplus opad) || H^s_{IV}((k \oplus ipad) || m)}$

This construction uses two arbitrarily chosen fixed constants opad and ipad. These are n length strings. The string opad is formed by repeating the byte x36 as many times as needed and the string ipad is formed by repeating the byte x5C in the similar way.

A key k is XORed with the ipad. The XORed result and the initialisation vector (0^n) are fed into the fixed length hash function h^s. The result obtained serves as the input for the next stage. In the next stage, a block of message m is used as the other input. These two inputs are again fed into h^s and so on. In the end the length of m serves as the input. The final output obtained from the subsequent steps will be fed again into the h^s along with another input $h^s(k \oplus opad, IV)$. The result is our HMAC tag.