HMAC

Def^n :- It consists of a message authentica^n code using hashing function.

Prop:- Since, the hashing functions tobe used in here are provably secure (Merkle Damgard and collision resistant function).

HMAC is automatically provable secure.

HMAC tag for m

$$m = H^{s}_{IV}((K \oplus opad) \| H^{s}_{IV}((K \, ipad) \| m))$$

This technique is the industry standard & used for designing algorithms