*MAC (Message authentication code).*

También conocido como “MAC” ó bien traducido al español como Código de Autenticación de Mensaje, es una porción de información utilizada para autenticar un mensaje.

Los valores MAC se calculan mediante la aplicación de una [función hash criptográfica](http://es.wikipedia.org/wiki/Funci%C3%B3n_hash_criptogr%C3%A1fica) con clave secreta *K*, que sólo conocen el remitente y destinatario, pero no los atacantes. Se dice que la función hash tiene que ser [criptográfica](http://es.wikipedia.org/wiki/Funci%C3%B3n_hash_criptogr%C3%A1fica) porque tiene que cumplir ciertas [propiedad de seguridad](http://es.wikipedia.org/wiki/Message_authentication_code#propiedad_de_seguridad) que las hacen resistentes frente ataques de adversarios.

*Tipos de funciones MAC.*

Actualmente, existen 3 grandes grupos de funciones MAC:

* **CBC-MAC**: La idea detrás de este algoritmo es la de convertir un algoritmo de cifrado simétrico en una función MAC. El funcionamiento básico consiste en cifrar el mensaje usando un algoritmo en modo CBC y tirar todo el resultado de texto cifrado a excepción del último bloque.
* **HMAC**: Dado que una función MAC es un mapeo aleatorio, y que las funciones hash se comportan como tales, podemos explotar la idea de utilizar una función hash para implementar una función MAC. La opción más popular hoy en día es la de usar HMAC-SHA-256.
* **UMAC**: Las funciones UMAC parten de la premisa de que el atacante necesita interactuar con el sistema para comprobar si el resultado MAC que ha generado es válido o no. Es decir, no existe nada parecido a un ataque exhaustivo off-line contra las funciones MAC. Así, argumentan que se puede reducir el resultado a tan solo 64 bits. Sin embargo, no existe un estándar bien definido de funciones MAC como ocurre con las funciones hash, lo que tiene efectos contraproducentes a largo plazo desde el punto de vista de la implementación.