1.

MD5: Sigue siendo usado, principalmente para confirmar la integridad de un archivo. Ya no se usa en muchos campos ya que no es muy seguro.

SHA-2 (256, 384, 512): Se siguen usando en varios campos. Se usan en múltiples protocolos como TSL, SSH entre otros, también es usado en los sistemas unix para el hasheo de las contraseñas. Las cripto monedas también usan este algoritmo para funcionar.