1. Ambos os esquemas criptográficos visam garantir a mesma propriedade de segurança: a autenticidade da mensagem e fazem-no, produzindo do lado do emissor qualquer coisa que é transmitida com a mensagem (no caso do mac uma marca, no caso da assinatura digital uma assinatura) e do lado do recetor essa “coisa” é verificada, confirmando ou desmentindo a autenticidade da mensagem. Diferem quanto à operação privada, já que no esquema MAC, todos podem verificar, e apenas o emissor autorizado pode gerar a marca. Assinatura digital o que é assinado é o resultado de uma função de hash
2. A organização da função de hash reduz uma mensagem com m bits a um bloco de n bits. A dimensão de yL = dimensão de m1, ou seja n bits = dimensão de um bloco <<< dimensão da mensagem, pelo que existe m e m’ tal que H(m) = H(m’)

Desenhar diagrama

1. Apesar de não ter acesso ao texto em claro, o que facilitaria o ataque, o atacante tem acesso ao texto cifrado. Sabendo que os mesmos blocos de texto em claro produzem as mesmas cifras, então um oráculo de encriptação pode ser usado. Se o atacante pode submeter texto em claro para encriptação, então também pode verificar hipóteses sobre o texto em claro que corresponde ao texto cifrado.
2. DES – 56 AES – 128 ???