1. Se o atacante conseguir que o resultado da passagem de duas mensagens distintas (x e x’) na função de hash seja igual, então este estaria na condição de conseguir forjar uma assinatura digital fazendo-se passar por outra pessoa.

Se T é um esquema MAC logo:

* ***m*** passará por um canal inseguro e será possível interceptar este valor.

Ao aplicar E já sabemos qual é:

* a sua chave: ***T(k1)(m)***
* e a sua mensagem: ***m*** (devido a esta passar em T no seu canal inseguro)

Com estes dois valores conhecendo algoritmo **E** conseguimos decifrar o seu resultado.

Desta forma estando na posse de ***T(k1)(m)*** e ***Es(T(k1)(m)1::L)(m)*** e fazendo a sua concatenação bit a bit obtém-se o criptograma CI(m). Por este meio prova-se que CI não é fiável para ser um criptograma de autenticidade visto que é possível ser quebrado.

* 1. Ver esquema folha rascunho

1. **o que é o texto em claro?**
2. Neste modo de operação é possível realizar paralelização de trabalho na operação de cifragem visto que para cifrar o bloco seguinte não é necessário utilizar um resultado previamente obtido. No extremo oposto a este caso está o modo de operação CBC que para cifra um bloco *“i”* necessita conhecer o resultado da cifra do bloco *“i-1”* para realizar o *XOR* com o resultado do bloco Ep(k). Caso i=0 então o valor com o qual será realizado o *XOR* será o de um Vetor Inicial (IV).