Daren - Alice   Ryan - Bob

TLS - 1)   Bob $e = 17$ $q = 410491$ $p = 10453$

$Key_{AES} = 0110\ 0011\ 0110\ 0001$

$Key_{MAC} = 0111\ 0011\ 0111\ 0100$

$Key_{AES+MAC} = 01100011\ 01100001\ 0111\ 0011\ 0111\ 0100$

$= 1667330932$

$n = 4290862423$

$M_1 = [(Key_{AES}, Key_{MAC})^e \bmod n\ ,\ IV]$

$= [(1667330932)^{17} \bmod 4290862423,\ IV]$

$= [2622473665, IV]$

$d = e^{-1} \bmod(\text{Ø}(n)) = 1261894553$

$M_1^d \bmod n = 1667330932$

$M_2 = 00D558C2$

0011 0000 0011 0000

$M_3 = (0011\ 0000\ 0011\ 0000, Key_{mac}) = 0100\ 0001\ 0100\ 0101$

$= 16709$

$M_4 = Mod(16709, n)$^$d = 631976641$

$M_5 = aesenc(Key_{aes}, IV, M_4) = 0111\ 0101\ 1010\ 0111$

$M_6 = aesdec(Key_{mac}, M_2) = 0011\ 0010\ 1110\ 1011$

i) If their MAC Values match, the A Knows B sent it.

$M_3 = M_c$

ii) It shouldn't match, and Alice will Know it's not Bob

iii) No, since Eve doesn't Know any other values and can't send another message