Item 5.

(:)

Assinatura verdadeira sobre x e x não foi alterado $\Longrightarrow g^{e_1} \cdot T^{k_2} \bmod p \bmod q = g^{K} \bmod p \bmod q$

(:) $g^{x D^{-1}} \cdot g^{SCD^{-1}} \bmod p \bmod q$

(:) $D = (x + SC)K^{-1}$

$\Leftrightarrow$

$DK = X + SC \Leftrightarrow X = -SC + Dk$

$g^{(-SC+Dk)D^{-1}} \cdot g^{SCD^{-1}} \bmod p \bmod q =$

$= g^{k} \cdot g^{-SCD^{-1}} \cdot g^{SCD^{-1}} \bmod p \bmod q = g^{d} \bmod p \bmod q$