a) De berekening maakt gebruik van de geheime sleutel van Alice en die is alleen aan Alice bekend.  
b) Bob gebruikt zijn eigen privé-sleutel **{m,b}** en berekent **cbmod m = (tB)bmod m = t.**Vervolgens gebruikt hij de publieke sleutel van Alice **{n,A}** en berekent **tAmod n =(sa)Amod n = s**  
c) In de berekening bij de ontcijfering is de privé-sleutel van Bob nodig en die is alleen aan Bob bekend.