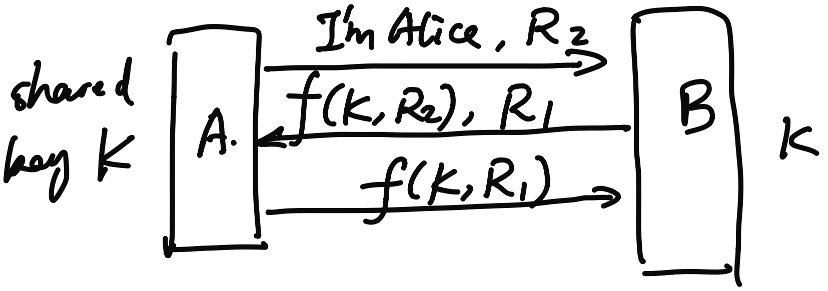
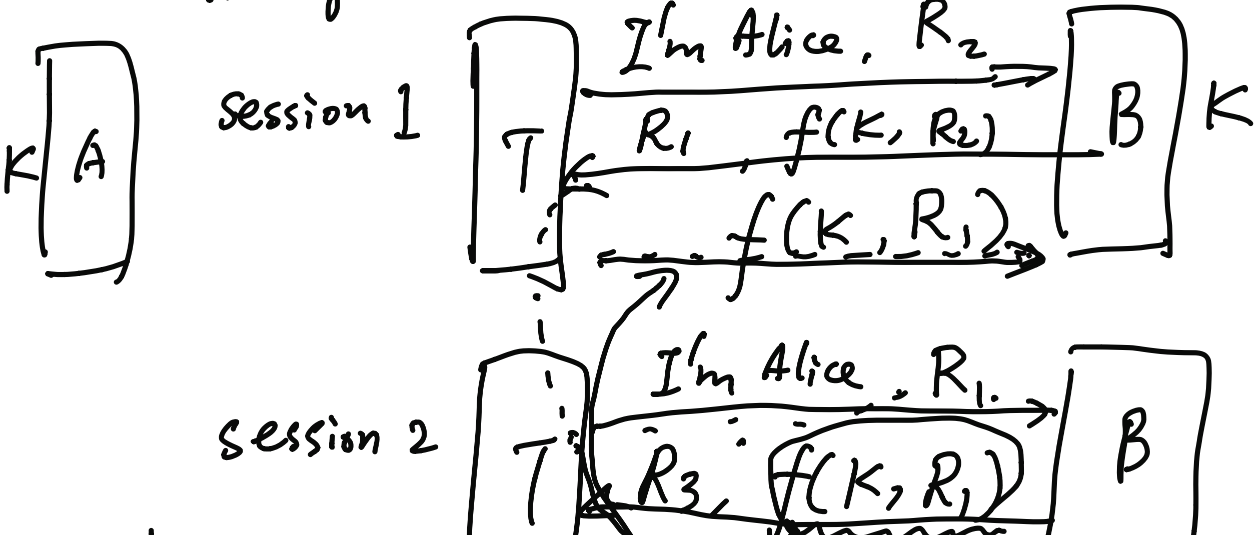
ECE 471/571 Authentication Protocols (cont'd)



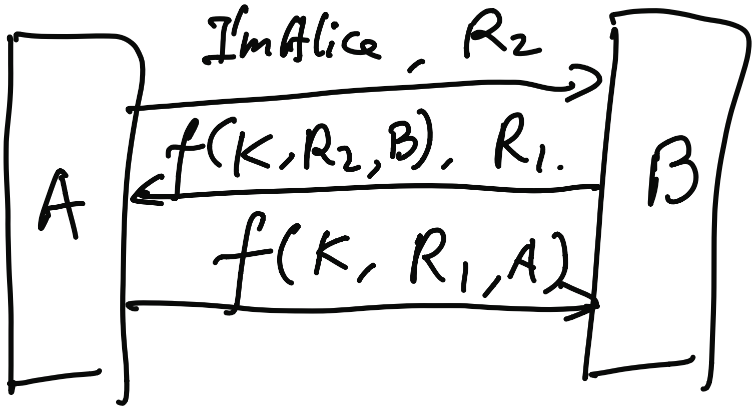
Reflection Attack. (parallel session)

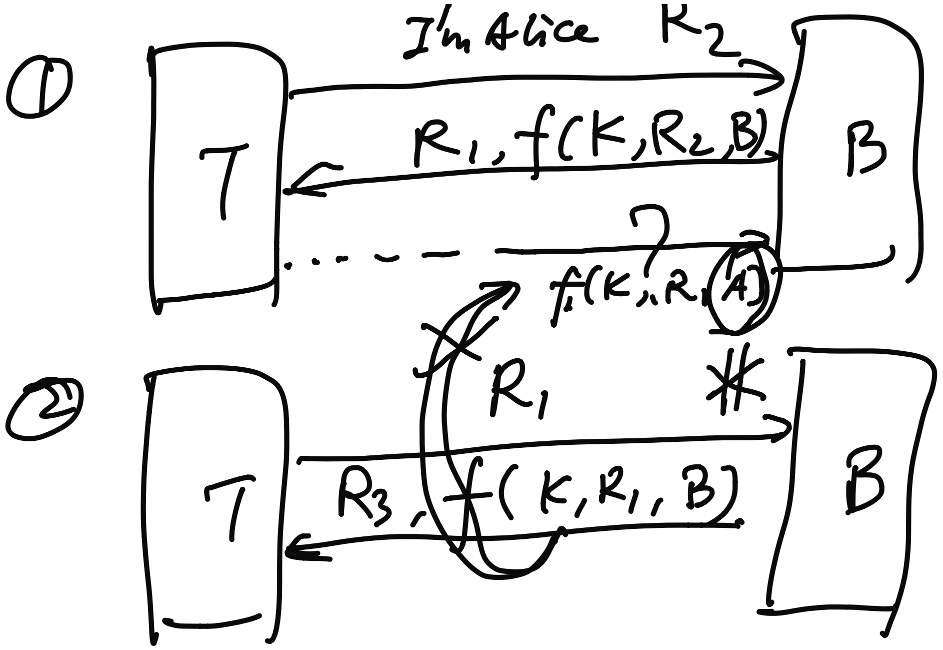
Trudy



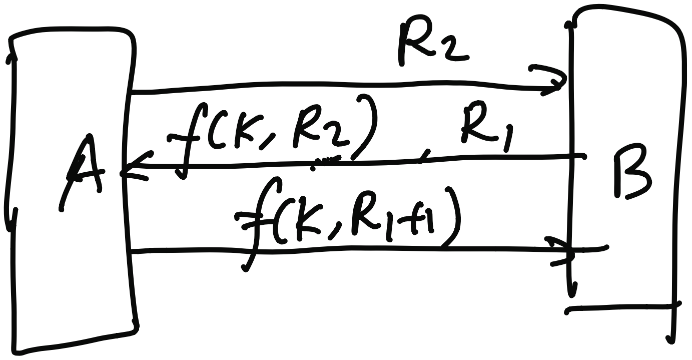
Solution:

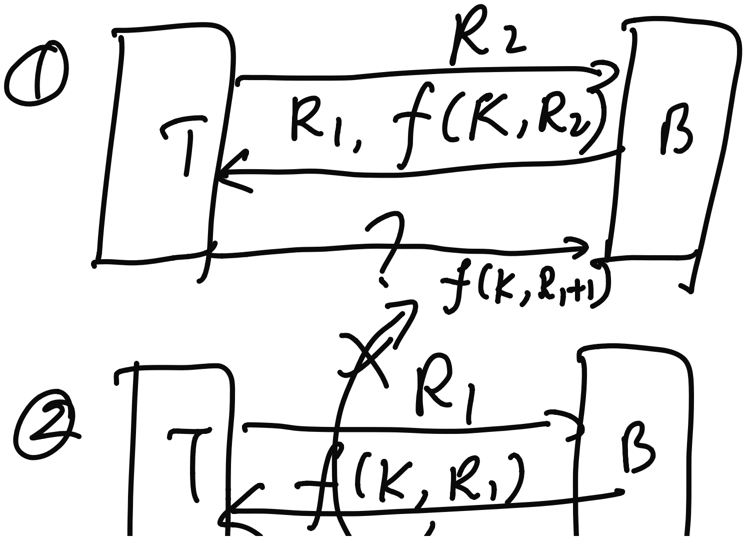
Different challenges/responses





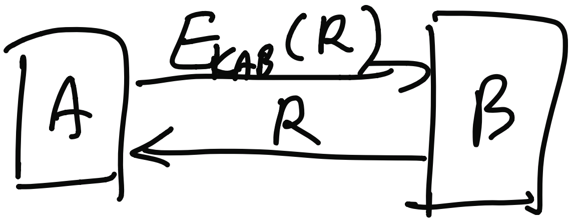
rule1: include IDs



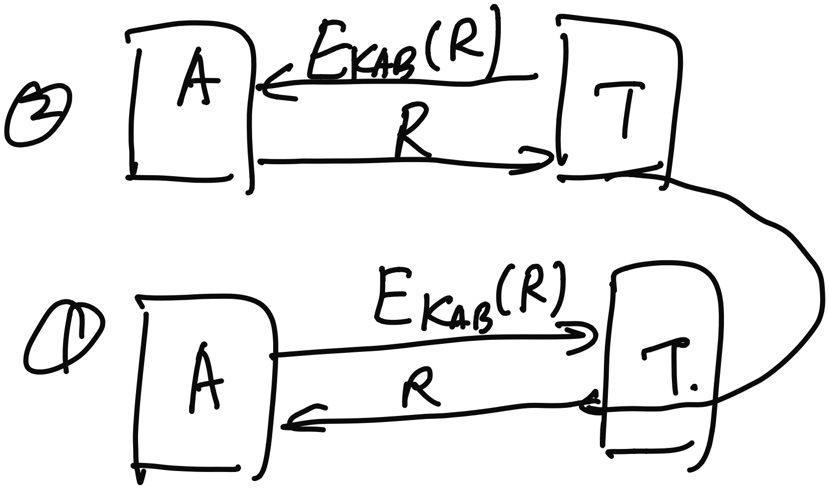


attack foiled

different format of response on each side



one-way authentication


②
A
$E_{K_{AB}}(R)$
R
T
①
A
$E_{K_{AB}}(R)$
R
T.