shared key K

I'm Alice, R_2

$f(K, R_2), R_1$

$f(K, R_1)$

A.   B   K

Reflection Attack.   (parallel session)

Trudy

K | A

Session 1

I'm Alice, R_2

$R_1, f(K, R_2)$

$f(K, R_1)$

T   B   K

Session 2

I'm Alice, R_1

$R_3, f(K, R_1)$

T   B

Solution:

Different challenges / responses

I'm Alice, R_2

$f(K, R_2, B), R_1$

$f(K, R_1, A)$

A   B

①
I'm Alice R_2
$R_1, f(K, R_2, B)$

T .... ? B
$f(K, R, (A)$

②
R_1 ✳
T $R_3, f(K, R_1, B)$ B

rule1: include IDs

R_2
$f(K, R_2), R_1$
A $f(K, R_1+1)$ B

①
R_2
T $R_1, f(K, R_2)$ B

? $f(K, R_1+1)$

②
R_1
T $f(K, R_1)$ B
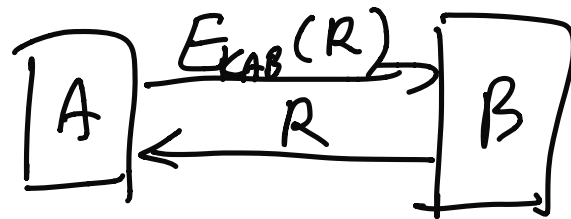
attack
foiled

different format of response on each side

one-way authentication

$A \xrightarrow{E_{K_{AB}}(R)} B$
$A \xleftarrow{R} B$

② $A \xleftarrow{E_{K_{AB}}(R)} T$
$A \xrightarrow{R} T$

① $A \xrightarrow{E_{K_{AB}}(R)} T$
$A \xleftarrow{R} T.$

$A \xleftarrow{R+1} B$
$A \xrightarrow{f(K, R+1)} B$