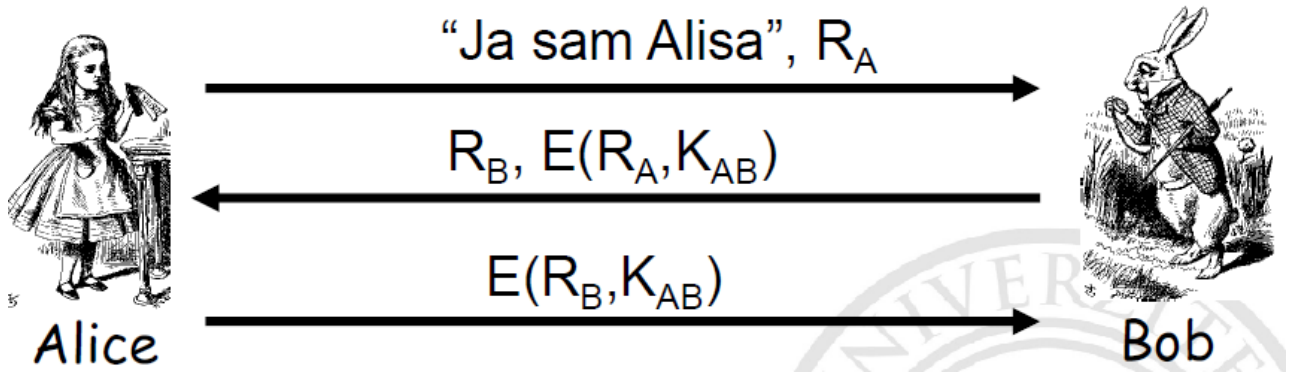
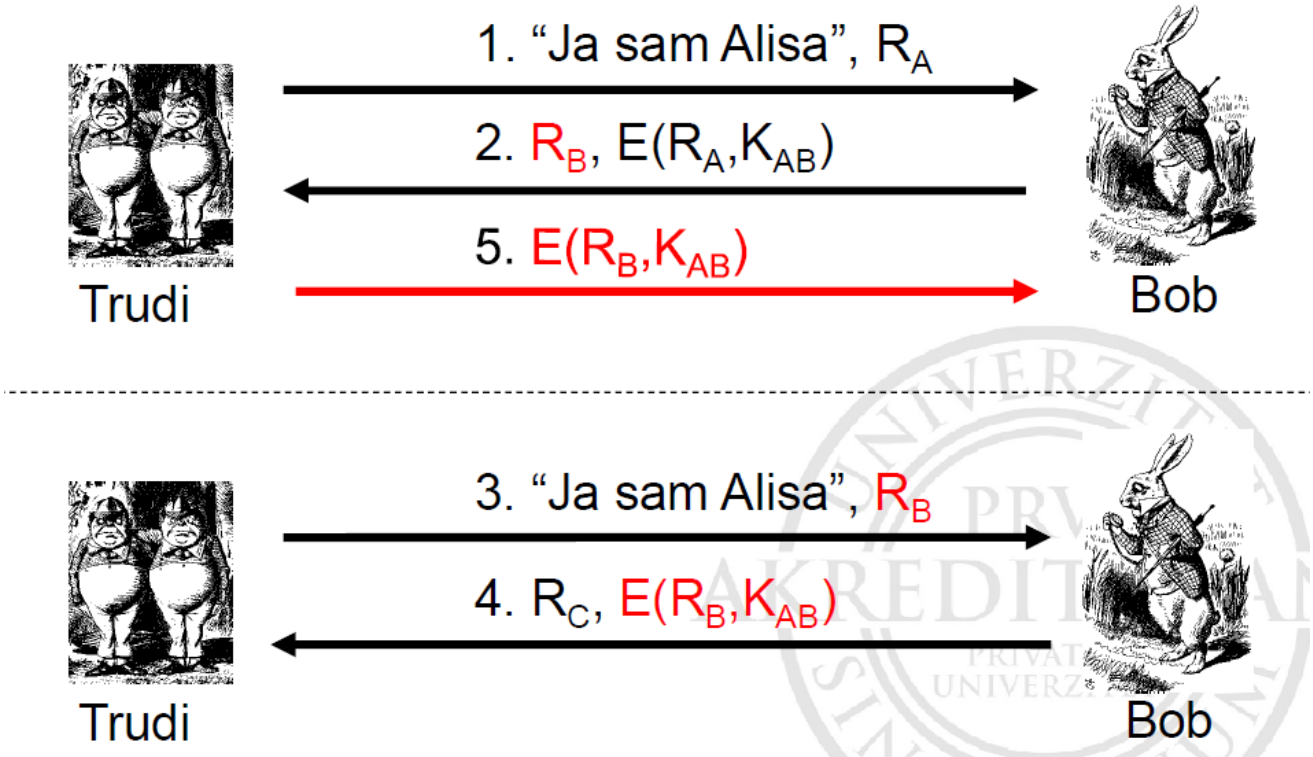


Slika 1 Aiutentifikacija simetričnim ključevima

1. Detaljno objasniti dizajn protokola sa slike 1.



Slika 2 Napad na protokol sa slike 1

2. Predložiti i objasniti modifikaciju koju je potrebno uraditi da bi se ova vrsta napada onemogućila, slika 2.
3. Nakon predložene modifikacije, objasniti sve promene koje bi postojale u slučaju da je zahtevano korišćenje vremenskog pečata (6 poena).
4. Prikazati samo jednu stranu komunikacije u Cryptool-u iz tačke 2.

Opis 1 (8 poena):

……

Opis 2 (8 poena):

…….

Opis 3 (6 poena):

……..

Opis 4 (8 poena).

……..

Napomena:

Na kraju rada, fajl prebaciti u mrežni folder **KOLOKVIJUM**, SREĆAN RAD!