3) SECURITY PROTOCOL

K = SHARED KEY

B capisce di star comunicando con A perchè solo A conosce K

La sicurezza di K è garantita, ovviamente se si utilizza un buon algo di cifratura simmetrica.

b)

B → A $\{B, T\}_K$

c) REPLAY ATTACK

d)