

# Security and Privacy, Blatt 0

Franziska Hutter, XXXXXXXX  
Felix Bühler, 2973410

18. April 2018

## Problem 1: Needham-Schroeder Protocol

## Problem 2: Another attack

Reflection attack:

Eine Person, die  $N_B$  korrekt entschlüsselt hat, ist jemand, der den KEY kennt (Alice). Allerdings kennt Bob selbst den KEY auch! Der Angreifer kann also die gesendeten Nachrichten aufzeichnen und später nochmal senden und sich damit als Alice ausgeben.

E = Evil (= Attacker)

1. Verbindung 1:  $A \rightarrow B$  :  $enc_s^k(N_A)$
2. Verbindung 1:  $B \rightarrow A$  :  $enc_s^k(N_B), N_A$
3. Verbindung 1:  $A \rightarrow B$  :  $N_B$
  
4. Verbindung 2:  $E \rightarrow A$  :  $enc_s^k(N_B)$
5. Verbindung 2:  $A \rightarrow E$  :  $enc_s^k(N'_A), N_B$
6. Verbindung 3:  $E \rightarrow A$  :  $enc_s^k(N'_A)$
7. Verbindung 3:  $A \rightarrow E$  :  $enc_s^k(N''_A), N'_A$
8. Verbindung 2:  $A \rightarrow E$  :  $N'_A$

## Problem 3: Woo and Lam Mutual Authentication Protocol