= Seminar 1 =

BAN → DEM. ÎN LOGICĂ
↳ LOGICĂ DEF. CA UN SI. DEDUCTIV

Needham Protocol: $A \to B: \{N_A, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_A^{-1}}$ } PERECHE ORDONATĂ
$B \to A: \{A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AB}}$

a) DPDV CRIPTOGRAFIC / AL SECURITĂȚII, PROTOCOLUL E CORECT?
R: NU (CU BAN-LOGIC, VA IEȘI "DA")

b) VERIFICARE CU BAN:

1) IDEALIZARE: ✓ (E DEJA)

2) ASUMPȚII: (1) $A \models A \overset{K_{AB}}{\leftrightarrow} B$ (2) $B \models \mapsto^{K_A} A$
(3) $B \triangleleft \{N_A, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_A^{-1}}$ (4) $A \triangleleft \{A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AB}}$
(5) $B \models A \Rightarrow (A \overset{K_{AB}}{\leftrightarrow} B)$
(6) $A \models \#(A \overset{K_{AB}}{\leftrightarrow} B)$
(7) $B \models \#(N_A)$

3) SCOP: $A \models B \models A \overset{K_{AB}}{\leftrightarrow} B$ și $B \models A \models A \overset{K_{AB}}{\leftrightarrow} B$ (MUTUAL AUTH.)

4) DERIVARE:

MM-PK $\dfrac{(2), (3)}{B \models (A \mid\sim (N_A, A \overset{K_{AB}}{\leftrightarrow} B))} \to (a)$

NC $\dfrac{(7)}{B \models \#(N_A, A \overset{K_{AB}}{\leftrightarrow} B)} \to (b)$

NV $\dfrac{(b), (a)}{B \models (A \models (N_A, A \overset{K_{AB}}{\leftrightarrow} B))} \to (c)$

BC $\dfrac{(c)}{B \models A \models A \overset{K_{AB}}{\leftrightarrow} B}$ ✓

MM-SK $\dfrac{(1), (4)}{A \models B \mid\sim (A \overset{K_{AB}}{\leftrightarrow} B)} \to (d)$

NV $\dfrac{(6), (d)}{A \models B \models (A \overset{K_{AB}}{\leftrightarrow} B)}$ ✓