= Seminar 4 =

1) Fie $f: Role \to Agents$, $f = \{i \to Alice; r \to Bob\}$

a) $\langle \theta, f, \emptyset \rangle (\{n_i, r\}_{pk(i)}) = ?$; $\theta \in RIS$, $T_\emptyset : Var \to RunTerm$

b) Match $(\langle \theta, f, \emptyset \rangle, \{n_i, r\}_{pk(i)}, \{n_i^{\#0}, Bob\}_{pk(Alice)}, \langle \theta, f, \emptyset \rangle)$.

a) ȘTIM CĂ $\langle \theta, f, \emptyset \rangle_{(R)} = f(R)$, DACĂ $R \in Role \cap dom(f)$

$\langle \theta, f, \emptyset \rangle (\{n_i, r\}_{pk(i)}) = \{\langle \theta, f, \emptyset \rangle (n_i, r)\}_{\langle \theta, f, \emptyset \rangle pk(i)} =$

$= \{\langle \theta, f, \emptyset \rangle_{n_i} \cdot \langle \theta, f, \emptyset \rangle_r\}_{\langle \theta, f, \emptyset \rangle pk(i)} = (n_i^{\#0}, Bob)_{pk(Alice)}$

b) "Match" ∈ ADEVĂRAT. AM DEM. LA "a" ↗ ȘI "=" AL 3-LEA TERMEN "Match" ✓

2) DEM. CĂ DIN $\Gamma = \{\{pk(i)\}_{sk(s)}, pk(s), \{nu\}_{sk(i)}\}$ SE POATE DEDUCE $\Gamma \vdash nu$.

$t \in \Gamma \Rightarrow \Gamma \vdash t$

ÎPOTEZE: $\Gamma \vdash \{pk(i)\}_{sk(s)}$, $\Gamma \vdash pk(s)$ $\} \to \Gamma \vdash pk(i)$

$\Gamma \vdash \{nu\}_{sk(i)}$ $\} \to \Gamma \vdash nu$ ✓

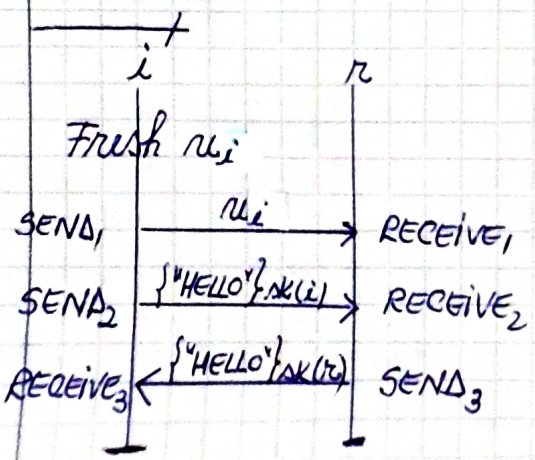
3) LABELLED TRANSITION SYSTEM (LTS): $(State, RunEvents, \to, \mathcal{A}_0(P))$

$State = \mathcal{P}(RunTerm) \times \mathcal{P}(Runs)$; $Runs = Insts \times RoleEvents^*$

$RunEvents = Insts \times (RoleEvents \cup \{create(R) \mid R \in Role\})$

$\mathcal{A}_i \xrightarrow{\alpha_{i+1}} \mathcal{A}_{i+1}$

$\mathcal{A}_0(P) = \ll AKN_0(P), \emptyset \gg$; $AKN_0(P)$ = INITIAL ADVERSARY KNOWLEDGE



a) $H(i)$; $H(r)$ — LEDGE

PROTOCOL (CURS 3, Pag 18, → "P")

b) AKN_0

c) runsof(H, i); runsof(H, r)

a) $H(i) = \{\{i, r, pK(i), sK(i), pK(r)\}, [SEND_1(i, r, n_i), SEND_2(i, r, \{\text{"HELLO"}\}_{sK(i)}), RECEIVE_3(i, r, \{\text{"HELLO"}, n_i\}_{sK(r)})]\}$

$H(r) = \{\{i, r, sK(r), pK(r), pK(i)\}, [RECEIVE_1(r, i, n_i), RECEIVE_2(r, i, \{\text{"HELLO"}\}_{sK(i)}), SEND_3(r, i, \{\text{"HELLO"}, n_i\}_{sK(r)})]\}$

b) $AKN_0 = \{i, r\} = Agents_H$

c) $runsof(H, i) = \{(\langle \theta, f, \tau \rangle, s) \mid s \in \Pi_2(H(i))\}$

$runsof(H, r) = \{(\langle \theta, f, \tau \rangle, s) \mid s \in \Pi_2(H(r))\}$