Exercise 11

donderdag 9 februari 2023 13:01

a) $A \to T$ (A, B)

$T \to A$ $(\{k_s\}_{K_A}, \{k_s\}_{K_B})$

step 3 is local

$A \to B$ $\{k_s\}_{K_B}$

step 5 is local

$A \leftrightarrow B$ $\{m\}_{K_S}$

not formally correct, split it up

b) $Init(A, B, net, k_A) ==$ out net (A, B); inp net x; split x in (x_1, x_2); new m; decrypt x_1 is $\{x_3\}_{K_A}$; out net $\{m\}_{x_3}$; inp net y; decrypt y is $\{y_1\}_{x_3}$;

out net x_2;

$Resp(A, B, net, k_B) ==$ inp net z; decrypt z is $\{z_1\}_{K_B}$; inp net w; decrypt w is $\{w_1\}_{x_1}$; new n; out net $\{n\}_{z_1}$;

$KDC(A, B, net, k_a, k_b) ==$ inp net p; if $(p = (A, B))$ then new k_s; out net $(\{k_s\}_{K_A}, \{k_s\}_{K_B})$

$System(net, A, B) ==$ new k_a, k_b; $(!KDC(A, B, net, k_a, k_b) \,||\, !KDC(B, A, net, k_b, k_a)) \,||\, !Init(A, B, net, k_A) \,||\, !Init(B, A, net, k_B) \,||\, !Resp(A, B, net, k_B) \,||\, !Resp(B, A, net, k_A))$