Exercise 10

donderdag 9 februari 2023 13:01

$A \to B$ (M, A)

$B \to A$ R

$A \to B$ $\{|\#(M,B)|\}_{sA}$

signatures are represented as encryptions, where the encryption key is secret and the decryption key is public.

$fnd(A, s_A, M, ret)$ = out ret (M,A); inp ret x; out ret $\{|\#((M,B))|\}_{sA}$;

$Recv(a, R, ret, B, v_A)$ = inp ret y; split y in (y_1, y_2); if $(y_2 = a)$ then out ret R; inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((y_1, B)))$ then stop

(v_A: verification key for A)

$system_A(A, B, M, ret, R)$ = new k_A; $(!\,\text{out ret } Rec(k_A);\ |\ !\,fnd(A, Enc(k_A), M, ret);\ |\ !\,Recv(A, R, ret, B, Rec(k_A)))$

$intruder_I(M, A, net)$ = inp ret x; out ret x; out ret (M,A); inp ret y; out ret x;

P == $system_A$ | intruder

== new k_A; (leave this parallel step out, since we do not need it: $!\,Rec(k_A) \mid !\,fnd(..) \mid !\,Recv(..)$) out ret (M,A); inp ret x; out ret $\{|\#((M,B))|\}_{sA}$; inp ret y; split y in (y_1, y_2); if $(y_2 = a)$ then out ret R; inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((y_1, B)))$ then stop | inp ret x; out ret x; out ret (M,A); inp ret y; out ret x;

≡ new k_A; (!!! out ret (M,A); inp ret x; out ret $\{|\#((M,B))|\}_{sA}$; inp ret y; split y in (y_1, y_2); if $(y_2 = a)$ then out ret R; inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((y_1, B)))$ then stop | inp ret x; out ret x; out ret (M,A); inp ret y; out ret x;

→ new k_A; (!!! inp ret x; out ret $\{|\#((M,B))|\}_{sA}$; split (M,A) in (y_1, y_2); if $(y_2 = a)$ then out ret R; inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((y_1, B)))$ then stop | inp ret x; out ret x; out ret (M,A); inp ret y; out ret x;

→ new k_A; (!!! inp ret x; out ret $\{|\#((M,B))|\}_{sA}$; if $(A = a)$ then out ret R; inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((M,B)))$ then stop | inp ret x; out ret x; out ret (M,A); inp ret y; out ret x;

→ new k_A; (!!! inp ret x; out ret $\{|\#((M,B))|\}_{sA}$; out ret R; inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((M,B)))$ then stop | inp ret x; out ret x; out ret (M,A); inp ret y; out ret x;

→ new k_A; (!!! out ret $\{|\#((M,B))|\}_{sA}$; inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((M,B)))$ then stop | inp ret x; out ret x; out ret (M,A); inp ret y; out ret x;

→ new k_A; (!!! stop | inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((M,B)))$ then stop | out ret $\{|\#((M,B))|\}_{sA}$; out ret (M,A); inp ret y; out ret $\{|\#((M,B))|\}_{sA}$;

→ new k_A; (!!! inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((M,B)))$ then stop | out ret $\{|\#((M,B))|\}_{sA}$; out ret (M,A); inp ret y; out ret $\{|\#((M,B))|\}_{sA}$;

→ new k_A; (!!! decrypt $\{|\#((M,B))|\}_{sA}$ is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((M,B)))$ then stop | out ret (M,A); inp ret y; out ret $\{|\#((M,B))|\}_{sA}$;

→ new k_A; (!!! if $(\#((M,B)) = \#((M,B)))$ then stop | out ret (M,A); inp ret y; out ret $\{|\#((M,B))|\}_{sA}$;

→ new k_A; (!!! | stop | out ret (M,A); inp ret y; out ret $\{|\#((M,B))|\}_{sA}$;

≡ new k_A; (!!! inp ret y; split y in (y_1, y_2); if $(y_2 = a)$ then out ret R; inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((y_1, B)))$ then stop | out ret (M,A); inp ret y; out ret $\{|\#((M,B))|\}_{sA}$;

→ new k_A; (!!! split (M,A) in (y_1, y_2); if $(y_2 = a)$ then out ret R; inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((y_1, B)))$ then stop | inp ret y; out ret $\{|\#((M,B))|\}_{sA}$;

→ new k_A; (!!! if $(A = a)$ then out ret R; inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((M,B)))$ then stop | inp ret y; out ret $\{|\#((M,B))|\}_{sA}$;

→ new k_A; (!!! out ret R; inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((M,B)))$ then stop | inp ret y; out ret $\{|\#((M,B))|\}_{sA}$;

→ new k_A; (!!! inp ret z; decrypt z is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((M,B)))$ then stop | out ret $\{|\#((M,B))|\}_{sA}$;

→ new k_A; (!!! decrypt $\{|\#((M,B))|\}_{sA}$ is $\{|z_1|\}_{v_A}$; if $(z_1 = \#((M,B)))$ then stop)

→ new k_A; (!!! if $(\#((M,B)) = \#((M,B)))$ then stop)

→ new k_A; stop !!!