Review question 14

zondag 19 februari 2023 02:39

Note that adding the identity of the sender and the receiver to the messages does not change anything in this protocol.
There are two main reasons for this:

1. The identities are known to the attacker;
2. A does not authenticate themselves.

This time, the protocol would look as follows in SPI calculus:

P = = new c ; out net $(A, B, \{|c|\}_{Enc(k)})$; inp net x; split x is (x_1, x_2, x_3); if $x_1 = B$ the if $x_2 = A$ the stop

Q = = inp net y; split y is (y_1, y_2, y_3); if $y_1 = A$ the if $y_2 = B$ then decrypt y_3 is $\{|z|\}_{Dec(k)}$; new n; (out net (B, A, n); secret (n))

R = = $P \mid Q$