Exercise 6

donderdag 9 februari 2023 13:01

$P == \text{new } C;\ \text{out net } \{|C|\}_{Enc(k)};\ \text{inp } c\ x;$

$Q == \text{inp net } y;\ \text{decrypt } y \text{ is } \{|z|\}_{Dec(k)};\ \text{new } n;\ \text{out } z\ n;$ (nonce)

$R == P \mid Q$

The nonce remains secret if Bob is certain the channel comes from Alice.

↓

in general, the attacker could have made the channel instead...