Exercise 5

donderdag 9 februari 2023 13:01

a) P == new k ; out net Enc(k);

P: process

b) Q = new k ; out net Enc(k); !(inp net M ; decrypt M is { x }_Dec(k) ; out net 'yeh')

c) Bob cannot receive his own public key; at the time he performs the out process (where the key is put out), he is not running any inp processes; hence, Bob cannot receive his own public key from net.

d) However, Bob can receive his own yeh messages; since he executes any number of inp ; decrypt ; out sequences in parallel, the 'yeh' message may end up in the inp process of another parallel execution. When this happens, the decryption will fail, and the process receiving the 'yeh' will then stop.

block