

DoubleNdeeProtocol











A

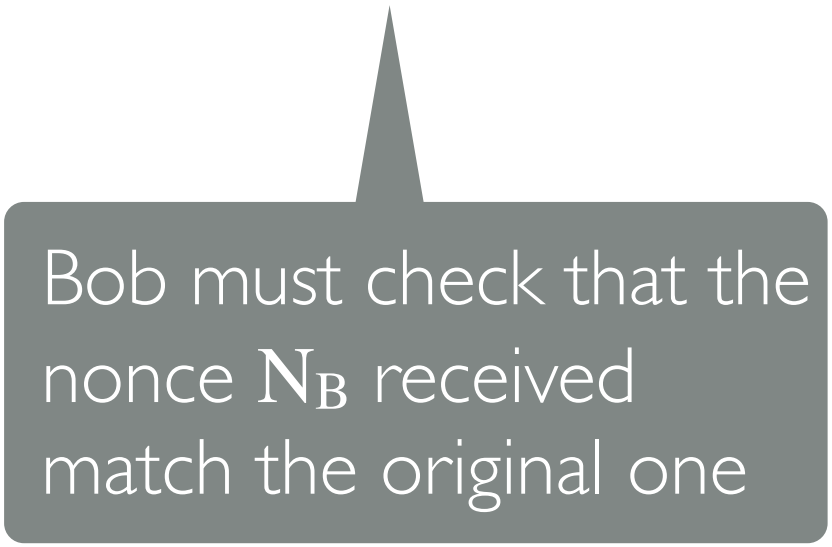


$$E_k(m, N_A, N_B)$$

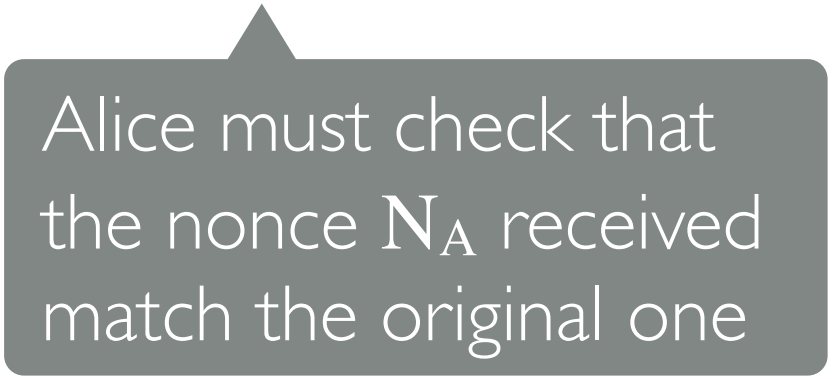

$$E_k(m', N_A)$$




$$E_k(N_B)$$

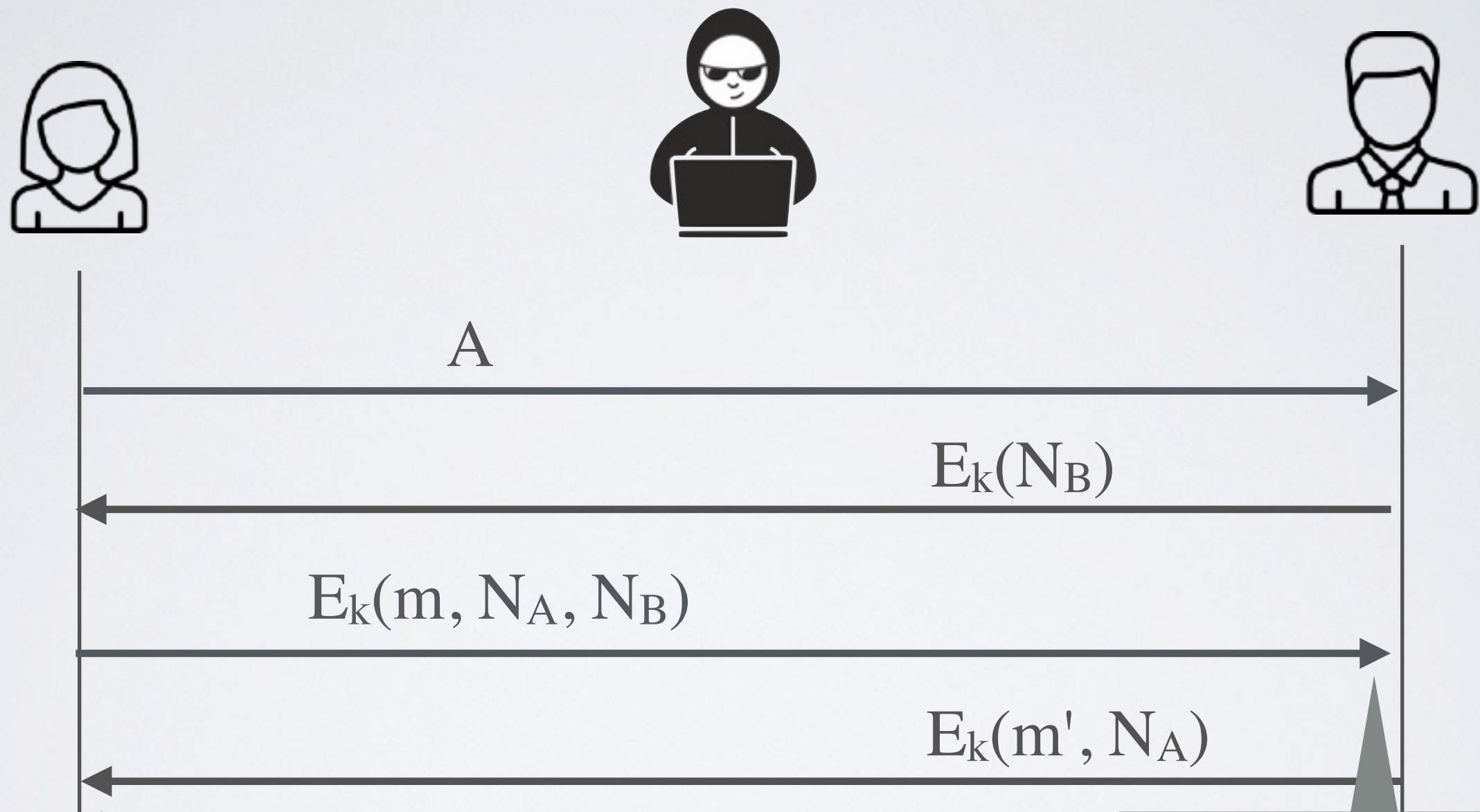


Bob must check that the
nonce N_B received
match the original one



Alice must check that
the nonce N_A received
match the original one

Double Nonce Protocol



Alice must check that the nonce N_A received match the original one

Bob must check that the nonce N_B received match the original one

Are we secure yet?

Two major issues:

1. **Key distribution**

If $A_1, A_2 \dots A_5$ want to talk, then $n \cdot (n-1) / 2$ keys must be exchanged physically using a secure channel

2. Does not ensure **Perfect-Forward Secrecy**

If somehow Mallory is able to compromise one of the participant at some point in time, she can decrypt all previous communications between Alice and Bob