4.3 The Man in the Middle

In this section we consider a communication protocol with asymmetric encryption, and note that the same attack works against the DIFFIE-HELLMAN key exchange. The basic problem is that an attacker can plant his own key into the procedure. In some more detail:

Suppose A = Alice and B = Bob want to exchange messages. First A sends her public key E_A to B, and B sends his public key E_B to A.

The attacker E = Eve who only listens cannot use these public data for eavesdropping. However the attacker M = Mallory, the "man in the middle" who actively forges messages, intercepts the key exchange, and each time replaces the intercepted public key by his own key E_M. From now on M is able to monitoring and even counterfeiting the complete communication of A and B. Figure 4.1 illustrates the attack.

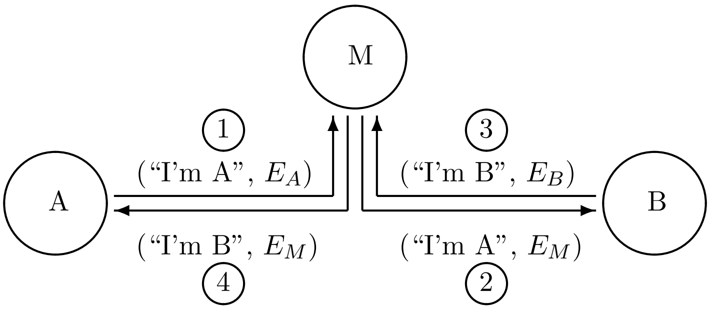

Figure 4.1: The man in the middle

There are different ways to prevent this attack. But all of them make asymmetric encryption more complex. The usual way is the use of certificates: The public keys of all participants of a communication network get a digital signature by a "trusted third party".

Definition. A certificate is a public key signed by a trusted third party.

Mnemonic. *A key exchange can be secure from the man in the middle only if the partners are mutually authenticated.*

Exercise. What information in the DIFFIE-HELLMAN protocol is suited to be used in a certificate?