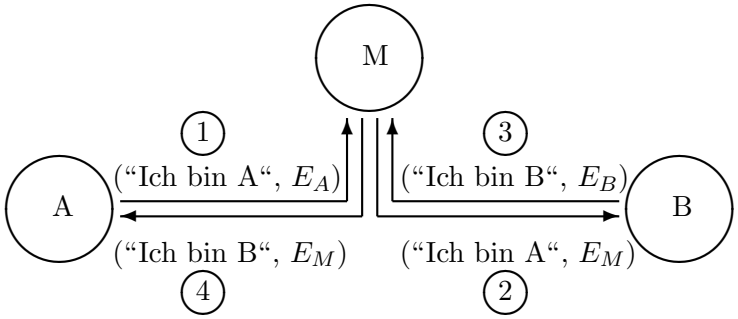
4.3 Der Mann in der Mitte

In diesem Abschnitt wird ein Kommunikationssystem mit asymmetrischer Chiffrierung betrachtet; für den DIFFIE-HELLMAN-Schlüsselaustausch funktioniert der Angriff genauso. Das Problem ist, dass ein Angreifer seinen Schlüssel in die Kommunikation einschleusen kann. Genauer:

A = Alice und B = Bob wollen miteinander kommunizieren. Dazu sendet A an B ihren öffentlichen Schlüssel E_A und B an A seinen öffentlichen Schlüssel E_B. Der Angreifer M = Mallory, der „Mann in der Mitte“, fängt diese Sendungen ab und ersetzt beide Male den abgefangenen öffentlichen Schlüssel durch seinen eigenen E_M. Dann kann M unbemerkt den ganzen Nachrichtenverkehr zwischen A und B abhören und sogar verfälschen; diese Situation ist in der folgenden Abbildung dargestellt.



Es gibt verschiedene Auswege aus dieser Bedrohung, die aber alle die asymmetrische Kryptographie verkomplizieren; der übliche Ausweg ist die Verwendung von Zertifikaten: Die öffentlichen Schlüssel aller Teilnehmer am Kommunikationsverfahren werden von einer bekannten und „vertrauenswürdigen“ Stelle – einem sogenannten Trustcenter – digital signiert. Zertifikat = öffentlicher Schlüssel mit digitaler Signatur des Trustcenters.

Merkregel. *Ein Schlüsselaustausch kann vor dem Mann in der Mitte nur sicher sein, wenn die Partner sich gegenseitig authentisieren können.*

Übungsaufgabe. Welche Information könnte man beim DIFFIE-HELLMAN-Verfahren als Zertifikat verwenden?