Authentizität

Ein wesentliches Ziel kryptographischer Verfahren ist Authentizität - man möchte sicher stellen, dass man tatsächlich mit dem richtigen Kommunikationspartner kommuniziert. Ist diese Verifizierung nicht möglich, kann ein Angreifer, der sich in einem günstigen Moment in den Kommunikationsvorgang einschaltet mit einem Man in the Middle Angriff (MITM) die scheinbar perfekt verschlüsselte Kommunikation mitlesen und sogar verändern: