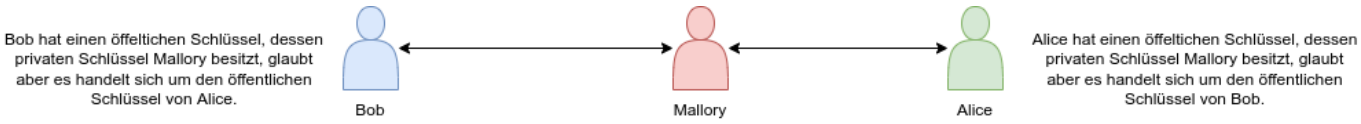
Authentizität

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.

Es ist wichtig zu verstehen, dass man wirklich sicher sein muss, dass ein öffentlicher Schlüssel, den man besitzt wirklich dem Kommunikationspartner gehört, den man als Besitzer betrachtet.

(A1)

Eine solche Situation kann beispielsweise eintreten, wenn man sich öffentlich Schlüssel von sogenannten "Keyservern" holt - man kann dann nicht mit Sicherheit sagen, ob ein öffentlicher Schlüssel der Person gehört, die dort angegeben ist.



- Was bedeutet in diesem Zusammenhang die Aussage "dieser öffentliche Schlüssel gehört Alice"?
- Welche Folgen hat die im Schaubild dargestellte Situation für die Vertraulichkeit der Kommunikation?
- In welcher Weise sind digitale Signaturen von dieser Situation betroffen?

Web of trust

GnuPG verfolgt zur Lösung des Authemtizitätsproblems einen dezentralen Ansatz, das sogenannte Web-of-trust. Dabei werden nach eingehender Prüfung die öffentlichen Schlüssel von Personen, die man beispielsweise auf einer Cryptoparty trifft von weiteren Schlüsselbesitzern mit deren privatem Schlüssel signiert.