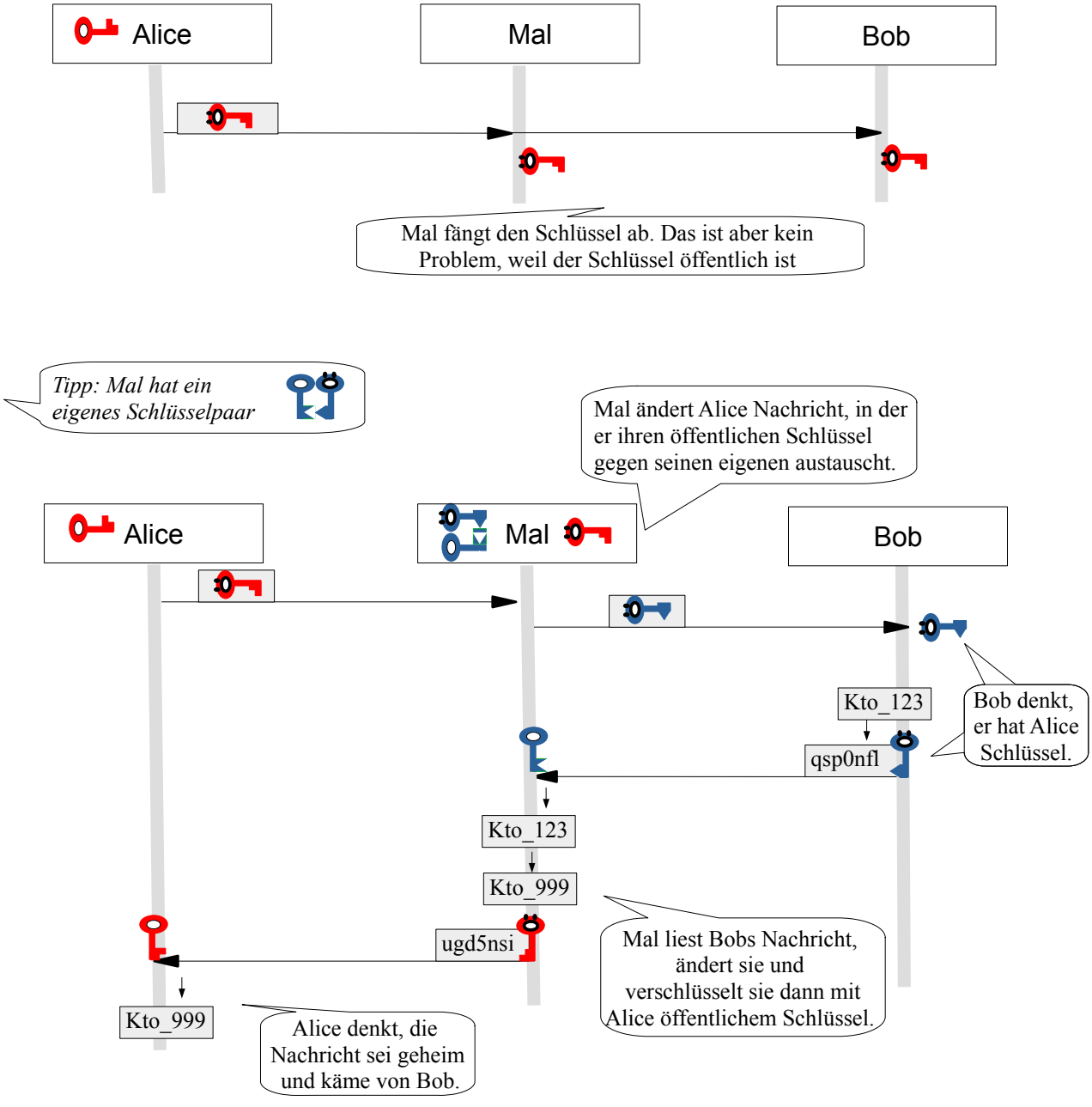
IuD: Man-in-the-middle-Angriff - Lösung

Aufgaben:

1.



2. Bobs Problem: Kommt der (öffentliche) Schlüssel wirklich von Alice? Die Authentizität ist nicht sichergestellt.

3. Man-in-the-middle-Angriff - indviduell (Aufgabe mit Chat-Tool)

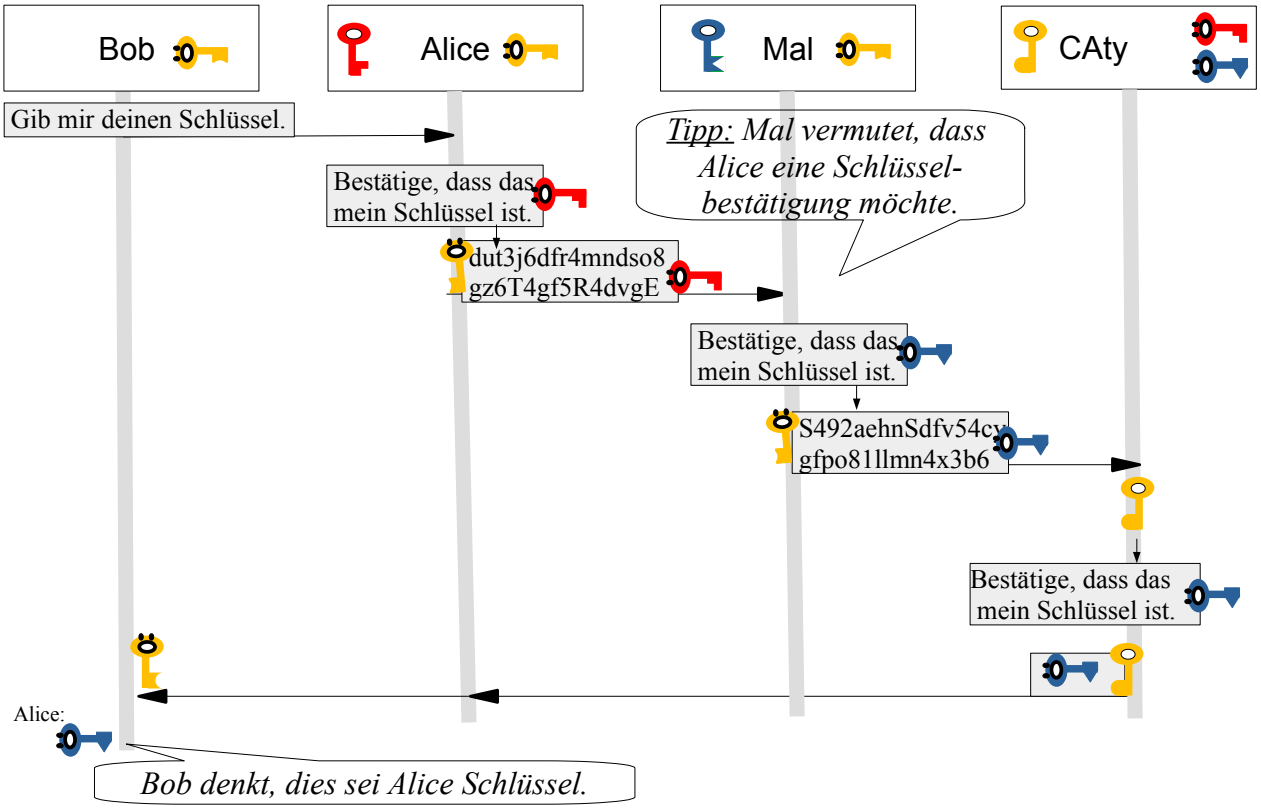
4. Ablauf: Bob fragt Alice nach ihrem öffentlichen Schlüssel. Alice bittet CAty zu bestätigen, dass es sich um Alice Schlüssel handelt. CAty wendet auf die Nachricht mit Alice Schlüssel ihren eigenen privaten Schlüssel an und schickt sie zu Bob. Bob wendet Catys öffentlichen Schlüssel an, verifiziert also die Nachricht und hat Alice öffentlichen Schlüssel.

a) Nein, nur CAty kann sie lesen, weil Alice sie mit CAtys öffentlichen Schlüssel verschlüsselt hat. Die Vertraulichkeit der Nachricht ist sichergestellt.

b) Mal kann die Nachricht, die Alice Schlüssel beinhaltet, lesen, weil er CAtys öffentlichen Schlüssel hat. Das ist aber nicht problematisch, da es sich um den öffentlichen Schlüssel von Alice handelt, den jeder haben darf.

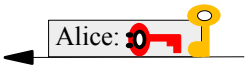
c) CAty wendet auf die Nachricht, die Alice Schlüssel beinhaltet, ihrem eigenen privaten Schlüssel an, um zu kennzeichnen, dass die Nachricht tatsächlich von CAty kommt. (Authentizität). Damit kann Bob sicher sein, dass die Nachricht von CAty stammt.

d) Nein, es ist nicht sicher:



Mal ändert Alice Nachricht und bittet um Bestätigung seines eigenen Schlüssels. Bob erhält eine Antwort, „verschlüsselt“ mit CAtys privatem Schlüssel. (Die Nachricht stammt ja auch von CAty, sie ist aber nicht die Antwort auf Bobs, bzw. Alice Frage.) Er ist sich nun sicher, dass er Alice Schlüssel hat. Nun kann Mal Bobs Nachrichten an Alice lesen und ändern. Weiterhin kann Mal in Bobs Namen Nachrichten an Alice schicken.

e) Statt nur den Schlüssel zu verschicken, wird der Name, also Alice, mitgeschickt.



Fordert Mal von CAty eine Schlüsselbestätigung und leitet diese an Bob weiter, so würde Bob die Vertauschung merken.