Keine Chance für Mal?

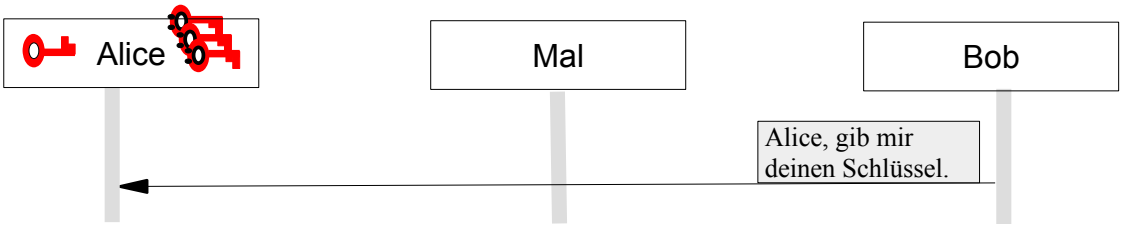
Hat Mal wirklich keine Chance, in die Kommunikation zwischen Alice und Bob einzugreifen?

Aufgabe:

1. *Suche nach der Schwachstelle. Spielt dazu mögliche Szenarien durch und notiert eure Beobachtung in Sequenzdiagrammen.*

   Das Szenario beginnt, bevor Alice ihren öffentlichen Schlüssel verteilt hat.

   (Fragt euren Lehrer ggf. nach einem Tipp.)



2. *Beschreibe, vor welchem Problem Bob steht?*

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

Startet pro Gruppe einmal das Programm ChatServerGUI.jar und startet den Server. Dann startet jeder das Programm ChatClient.jar.

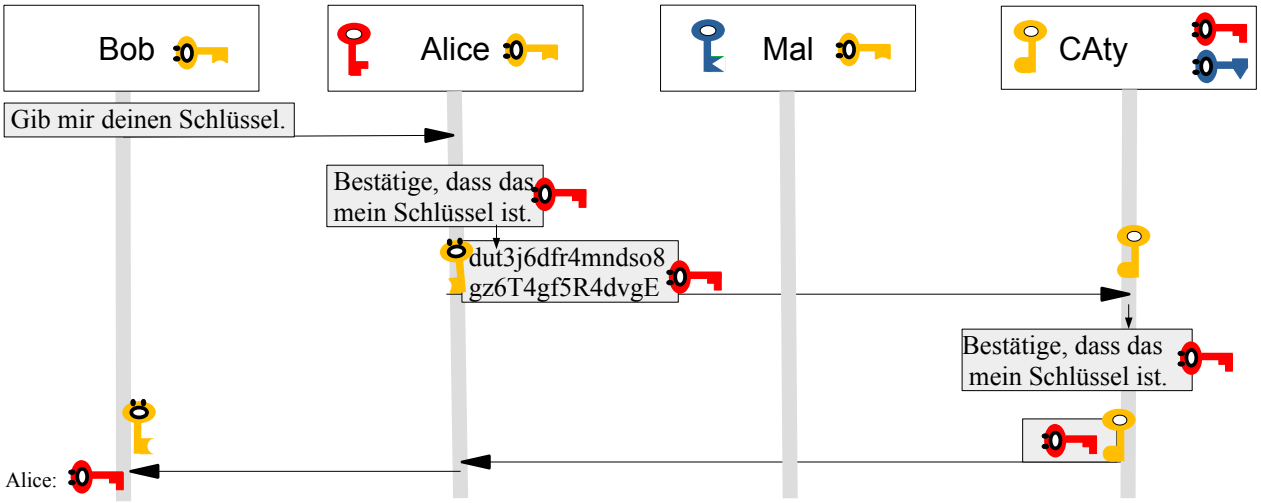
Mindestens zwei Personen wollen vertraulich miteinander kommunizieren. Sie erzeugen dazu ein Schlüsselpaar (Schlüssel noch nicht versenden). Eine dritte Person, Mal, der Man-in-the-Middle, verbindet sich ebenfalls mit dem Server und erzeugt ein Schlüsselpaar.

Spielt folgendes Szenario durch:

Der versendete öffentliche Schlüssel wird vom Man-in-the-Middle ausgetauscht. Nachfolgend kann er dann Nachrichten manipulieren. Dazu hat er folgende Möglichkeiten:

- *Er kann jede Nachricht aufhalten (Stop-Button).*
- *Er kann einen versendeten Schlüssel austauschen (rechte Maustaste auf die Schlüsselnachricht)*
- *Er kann eine Nachricht verändern (rechte Maustaste auf die Nachricht)*

4. *Betrachte folgenden Ablauf:*



a) Kann Mal die Nachricht, die Alice an CAty schreibt, lesen?

b) Kann Mal die Nachricht, die Alice Schlüssel beinhaltet, lesen?

c) Warum wendet CAty auf die Nachricht, die Alice Schlüssel beinhaltet, ihrem eigenen privaten Schlüssel an?

d) Ist dieses Szenario wirklich sicher? Spielt es durch und findet die Schwachstelle. (Fragt euren Lehrer ggf. nach einem Tipp.)

e) Wie kann man diese Schwachstelle beseitigen?