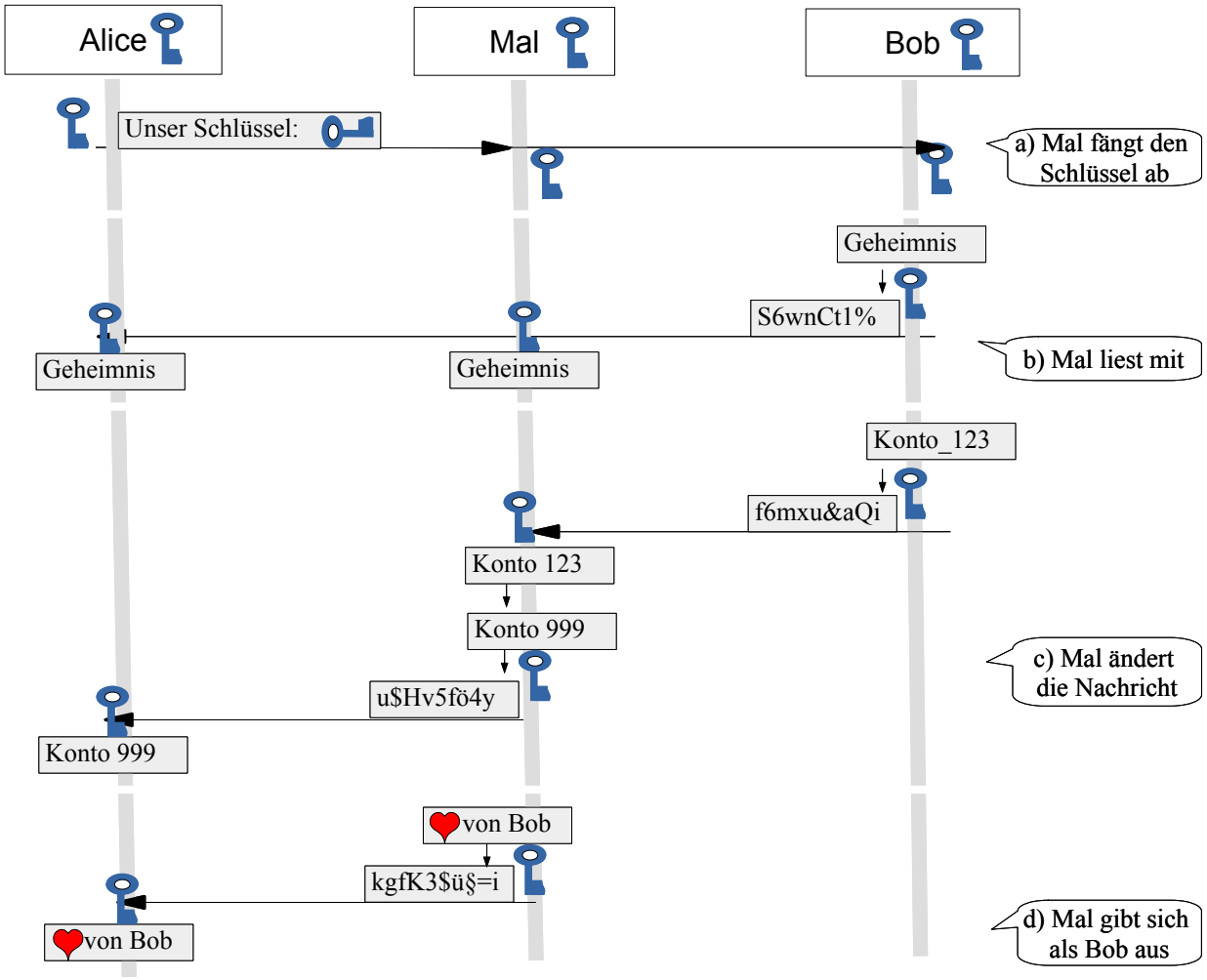
IuD: Kryptologie - Wiederholung - Lösung

Aufgaben:

1. Kryptoverfahren:

- Transpositionsverfahren
  - Skytale: sehr leicht zu brechen, da nur sehr wenige Schlüssel in Frage kommen.
- Substitutionsverfahren:
  - Cäsar: monoalphabetisch, sehr leicht zu brechen (nur 25 mögliche Schlüssel)
  - Allgemeine monoalphabetische Substitution: viele Schlüssel (25!), aber mit Häufigkeitsanalyse zu brechen.
  - Vigenère: polyalphabetisch, schwieriger zu brechen, aber mit zweistufigem Verfahren (Angriff auf Schlüssellänge, danach Häufigkeitsanalyse der Teiltexte) möglich.
  - One-Time-Pad: polyalphabetisch, absolut sicher, Nachteil: Schlüssel so lang wie die Nachricht, nur einmal verwendbar → Problem des Schlüsseltauschs
- Modernes Verfahren:
  - AES: Kombination aus Transposition und Substitution, nicht 100% sicher, aber zur Zeit ein praktikabler Kompromiss.

2.



3.

Angriffsmöglichkeit:	Krypto-Ziel:
Mitlesen der Nachricht	1. Vertraulichkeit
Ändern der Nachricht	2. Integrität
Absender fingieren	3. Authentizität *

* Das Ziel Verbindlichkeit wird hier nicht weiter differenziert.

4. Zentrales Problem ist der Schlüsseltausch.