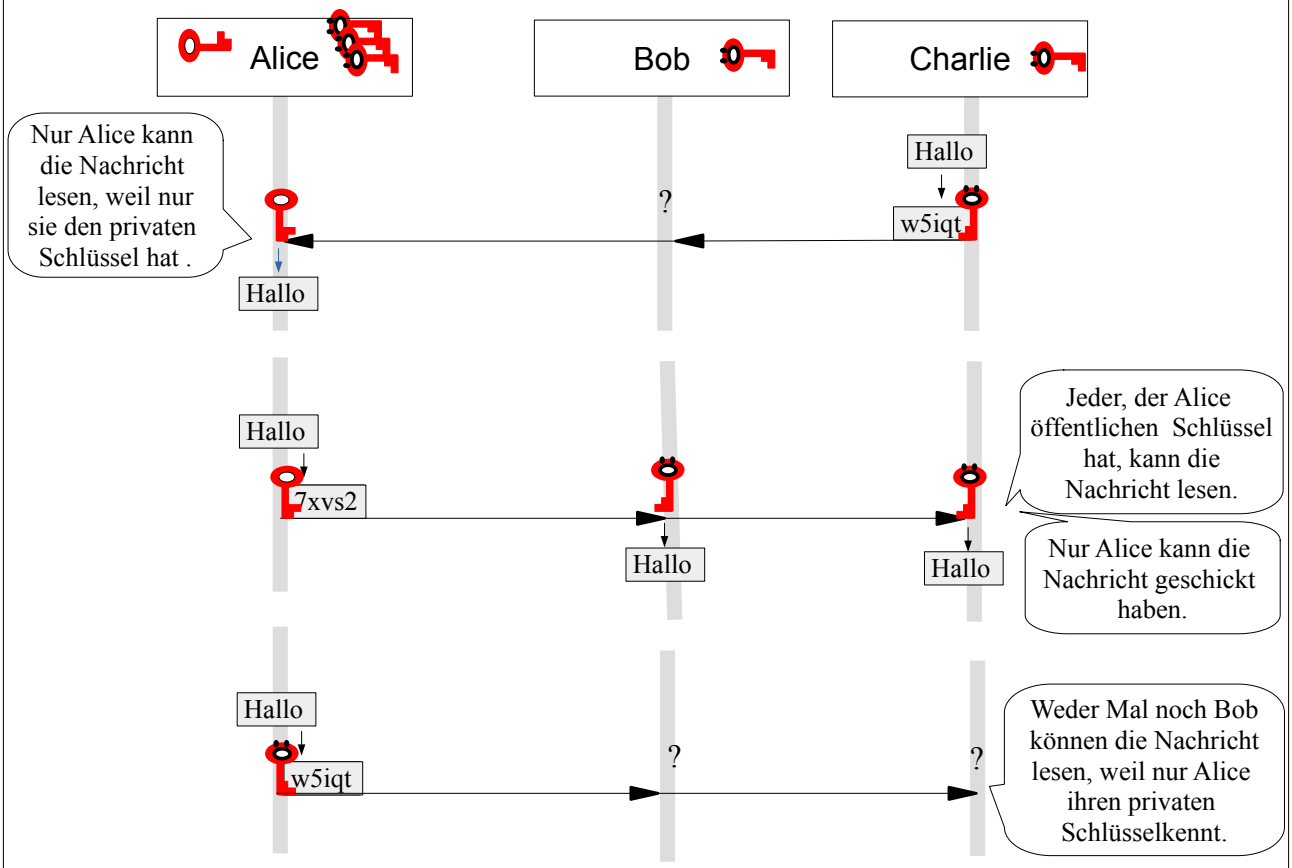
IuD: Asymmetrische Verschlüsselung - Lösung

Aufgaben:

1. Das Ver- und Entschlüssel sind symmetrisch: beide verwenden denselben Schlüssel. Beim asymmetrischen Verfahren sind beide Verfahren asymmetrisch, weil beide verschiedene Schlüssel nutzen.

2.



a) Jeder, der einen öffentlichen Schlüssel von Alice hat, kann ihr geheime Nachrichten schreiben.

b) Alice kann niemandem geheime Nachrichten schreiben.

c) B und C können nicht geheim kommunizieren.

3. a) Nachrichten an A: Krypto-Ziel der Vertraulichkeit.

b) Nachrichten von A zu irgendjemandem: Krypto-Ziel der Authentizität.

Bob kann nicht sicher sein, dass niemand sonst die Nachricht gelesen hat.

Bob kann sicher sein, dass die Nachricht von Alice kommt.

4.

	Asymmetrisch	Symmetrisch
a) Anzahl Schlüssel:	**5** Schlüsselpaare **n** Schlüsselpaare	4+3+2+1= **10** Schlüssel (n-1)+(n-2)+...+1 = **(n-1)·n : 2** Schlüssel (bei n= 100: 4950 Schlüssel)
b) Jeder verwaltet:	das eigene Schlüsselpaar sowie die öffentlichen Schlüssel der anderen, also: 4+2= **6 Schlüssel** n+1 Schlüssel	4 Schlüsssel n-1 Schlüssel

5. Verschlüsseln mit asymmetrischer Verschlüsselung: (Aufgabe mit Chat-Tool)

e) Verwendeter Schlüssel: der öffentliche Schlüssel des Empfängers

f) Verwendeter Schlüssel: mein privater Schlüssel

g) Verwendeter Schlüssel: mein privater Schlüssel

h) Verwendeter Schlüssel: der öffentliche Schlüssel des Absenders. Nur so kann ich sicher sein, dass der angegeben Absender die Nachricht geschrieben hat.