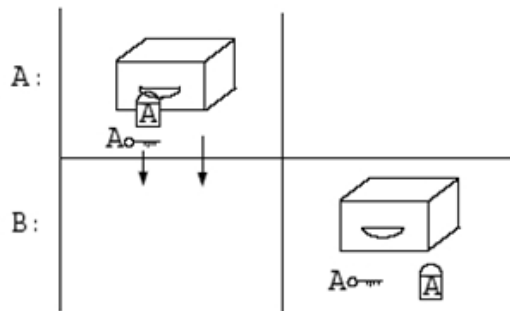


# Arbeitsblatt: Symmetrische und asymmetrische Verschlüsselung

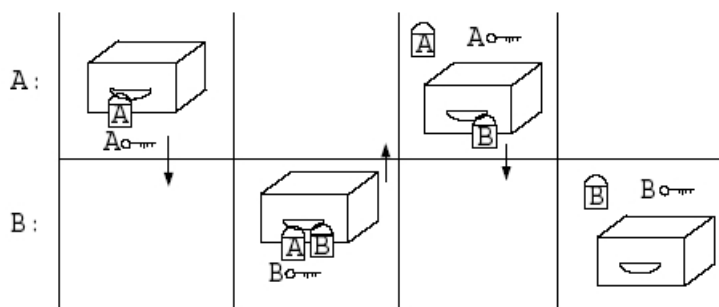
## Klassische Kryptographie – symmetrische Verschlüsselung



**Aufgabe 1:** Was ist der Nachteil an dieser Methode?

**Paradoxon:** Will man ein Geheimnis austauschen, muss man schon vorher ein Geheimnis ausgetauscht haben.

70er Jahre: neue Idee nach Whitfield Diffie & Martin Hellman asymmetrische Verschlüsselung:



**Aufgabe 2:** Fasse die Schritte in Worte!

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_

**Problem:** In der Kryptographie nimmt man an, dass das Ver-schlüsselungsverfahren nicht geheim gehalten werden kann, somit bietet nur ein einziger Schlüssel zum Ver- und Entschlüsseln keine Sicherheit.

**Lösungen:** Man verwendet asymmetrische Verschlüsselungen. Wenn der Schlüssel zum Verschlüsseln jedem zugänglich gemacht wird, also ein öffentlicher Schlüssel ist, befinden wir uns in der Public Key Kryptographie.

**Wichtig hierbei ist:** Aus dem Wissen über den Schlüssel für die Verschlüsselung darf man nichts über das Verfahren der Entschlüsselung herausbekommen!