Prinzip: Damit **Bob** an **Alice** eine verschlüsselte Nachricht schicken kann, muss Alice ein **Schlüsselpaar** aus **öffentlichem** und **privatem Schlüssel** erzeugen (berechnen). Bob verschlüsselt die Nachricht an Alice mit deren öffentlichen Schlüssel, Alice entschlüsselt mit ihrem privaten Schlüssel.

Geheimer Bereich von Alice	Öffentlicher Bereich	Geheimer Bereich von Bob
Alices Tätigkeiten: Wähle zwei verschiedene Primzahlen (dreistellig): **p=** ☐ **q=** ☐ Websuche: Tabelle der Primzahlen, auf Wikibooks Berechne **n = p*q =** ☐ **m = (p-1)(q-1) =** ☐ Wähle eine Zahl a, die zu m teilerfremd ist: **a =** ☐ Übertrage den **öffentlichen Schlüssel (n, a)** in den öffentlichen Bereich →	Öffentlicher Schlüssel von Alice: **n =** ☐ **a =** ☐	**Bobs** Tätigkeiten: Schreib eine **Nachricht** x als natürliche Zahl, die **kleiner als n** ist: **x =** ☐ Verschlüssle die Nachricht mit der Formel **$y = x^a \pmod n$** **y =** ☐ Hilfsmittel: Wolfram Alpha (im Web) Übertrage y in den öffentlichen Bereich (schicke sie an Alice)
↓ Berechne nun den **privaten Schlüssel (n, b)**: Ermittle b nach der Formel **$b * a \equiv 1 \pmod m$** (Suche **das kleinste Vielfache** von a, das beim Teilen durch m den Rest 1 ergibt, z. B. mit einer Tabelle oder Wolfram Alpha) **b =** ☐ Entschlüssle Bobs Nachricht mit der Formel **$x = y^b \pmod n$** **x =** ☐	Verschlüsselte Nachricht von Bob: **y =** ☐	↙