4) Textbook RSA

a)

Alice:

$$\boxed{\begin{array}{l} p = 11 \\ q = 17 \\ e = 13 \end{array}} \rightarrow N = p \cdot q = 187$$

$$\Rightarrow \varphi(N) = 10 \cdot 16 = 160$$

$d = ?$

$$\Rightarrow \quad e \cdot d = 1 \bmod \varphi(N)$$

$$13 \cdot d = 1 \bmod 160$$

1) $160 = 12 \cdot 13 + 4 \Rightarrow 4 = 1 \cdot 160 - 12 \cdot 13$

2) $13 = 3 \cdot 4 + \underline{1} \rightarrow \text{ggT} \Rightarrow 1 = 13 - 3 \cdot 4$

aus 1 in 2:

$$1 = 13 - 3 \cdot 4$$

$$1 = 13 - 3 \cdot (160 - 12 \cdot 13)$$

$$1 = 13 - 3 \cdot 160 + 36 \cdot 13$$

$$1 = -3 \cdot 160 + \boxed{37} \cdot 13$$

$\downarrow$ inverse $\underline{\underline{d = 37}}$

$$\underline{\underline{pk}} = (\overset{N}{187}, \overset{e}{13}) \quad , \quad \underline{\underline{sk}} = (\overset{N}{187}, \overset{d}{37})$$

4) Textbook RSA ctd.

b) Bob verschlüsselt

$pk = (187, 13)$

$m = 42$

$c = m^{e} \bmod \overset{N}{\cancel{N}}$

$\underline{\underline{c}} = \boxed{42}^{13} \bmod 187 = \underline{\underline{179}}$

c) Alice entschlüsselt

$c = 179$, $sk = (187, 37)$

$m = c^{d} \bmod N$

$\underline{\underline{m}} = 179^{37} \bmod 187 \boxed{= \underline{\underline{42}}}$

Korrekt ✓