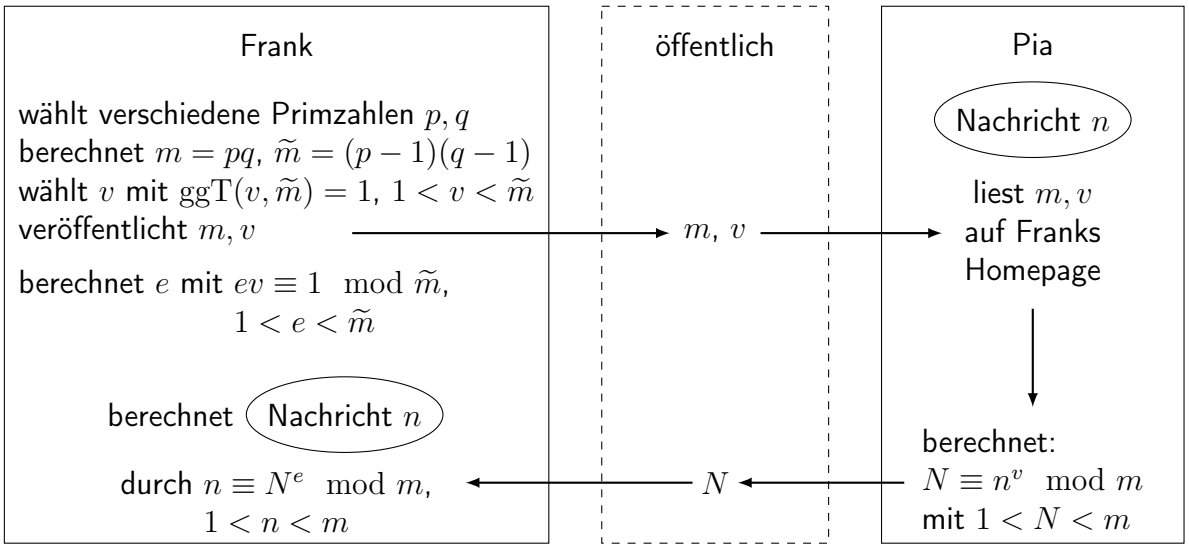
Das RSA-Verfahren

(von Rivest, Shamir, Adleman)



Aufgabe 3

Frank wählt: $p = 3$, $q = 11$,

berechnet: $m =$ $\widetilde{m} =$

wählt: Verschlüsselungsexponent $v = 7$ (erfüllt $1 < v < \widetilde{m}$ und $\mathrm{ggT}(v, \widetilde{m}) = 1$)

veröffentlicht: $m =$ und $v = 7$

berechnet: e:

Pia liest die Homepage von Frank und will ihm die Nachricht $n = 6$ übermitteln. Sie berechnet

Modulo 33: $n^v = 6^7 =$

und schickt Frank $N =$. Frank liest in Pias Mail $N =$ und berechnet

Modulo 33: $N^e =$

erhält also $n =$ zurück.