Feige–Fiat–Shamir Proof of Identity:

- *the best–known zero–knowledge* protocol
- asym. Algorithmen nutzen

Ziel: Peggy gegenüber Terminal authentisiert

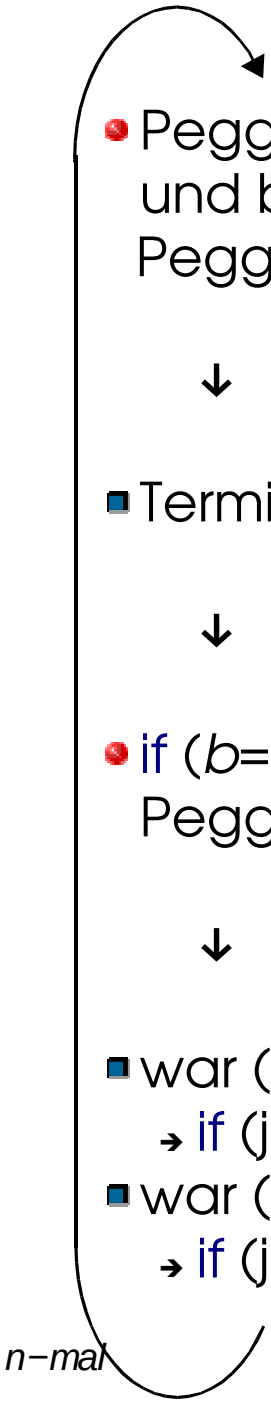
Voraussetzung:
asym. Schlüssel generiert

- public v
- privat s

} für Peggy

mit: n Zufallszahl (512...1024bit), Primprodukt
$x^2 = v \mod n$
$v^{-1} \mod n$ existiert
$s = \text{sqrt}(1/v) \mod n$

Protokoll:



- Peggy erzeugt Zufallszahl r (Bedingung: $r<n$) und berechnet $x = r^2 \bmod n$
  Peggy sendet x an Terminal

↓

- Terminal sendet zufälliges bit b={0,1} an Peggy

↓

- if (b=0) Peggy sendet r zum Terminal else
  Peggy sendet $y=r*s \bmod n$ zum Terminal

↓

- war (b=0) überprüfe $x=r^2 \bmod n$
  - → if (ja) Peggy kennt sqrt(x)
- war (b=1) überprüfe $x=y^2 * v \bmod n$
  - → if (ja) Peggy kennt sqrt(x/v)

n−mal