

(e,d; n) erzeugen
(durch Schlüsselzentrale)

(d,n): privater Schlüssel

(e, n): öffentlicher Schlüssel

m

Signatur für m erzeugen
 $\text{sig} = m^d \bmod n$

m

sig

sig verifizieren
 $\text{sig}^e \bmod n \stackrel{!}{=} m$