RSA-Signaturen

- RSA-Signatur: $S = M^e \bmod N$
- M: Eingabe; N, e: Private Key
- RSA wird nie „roh“ eingesetzt, M!=Nachricht
- Signiert wird nach einer Codierung der Nachricht, z. B. mit Hash-Funktion (PKCS #1 1.5)
- Keine bekannten Angriffe, aber Sicherheit nicht „beweisbar“

RSA-PSS

- Probabilistic Signature Scheme: Sicherheit beweisbar auf RSA/Hash-Funktion rückführbar.