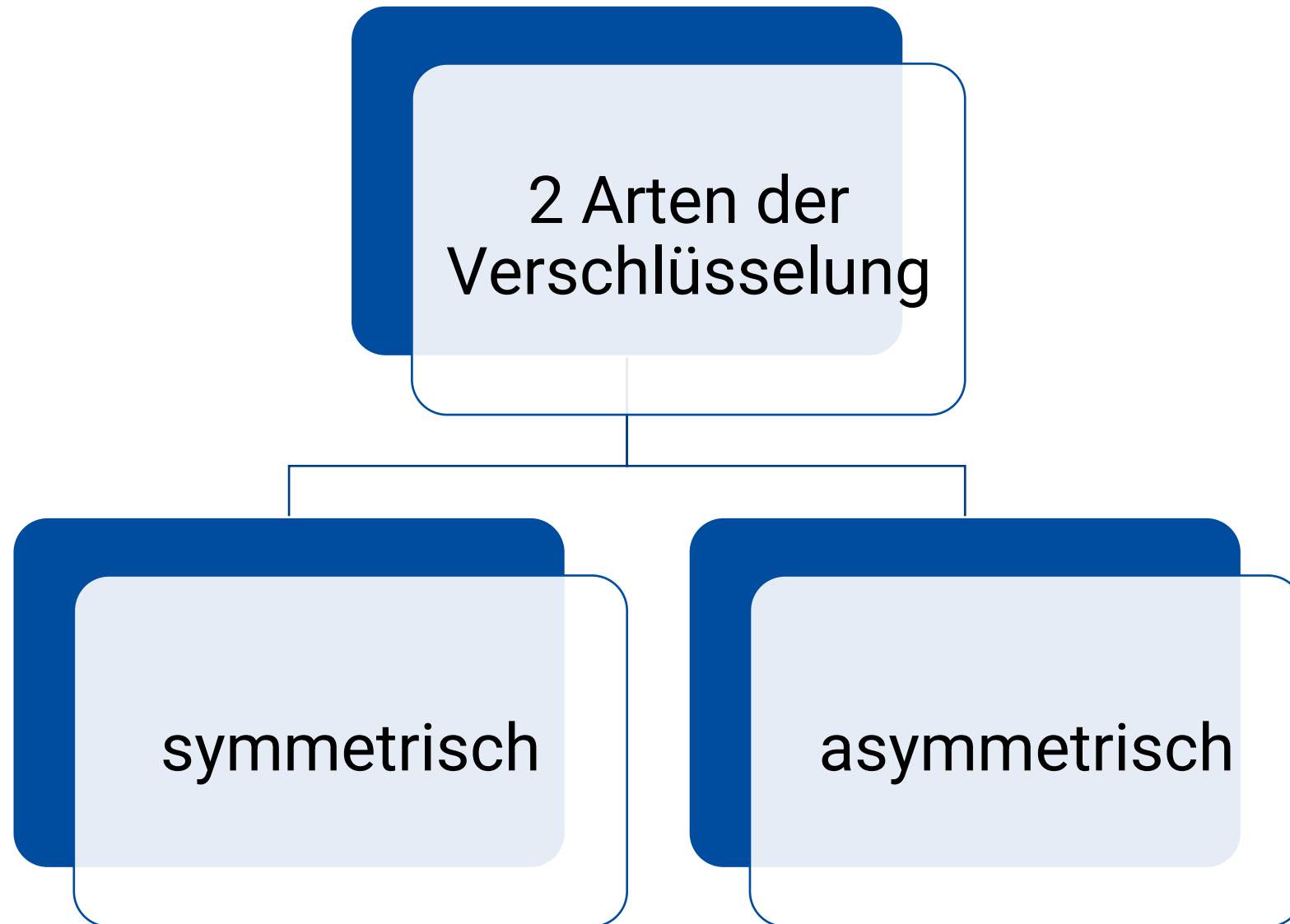
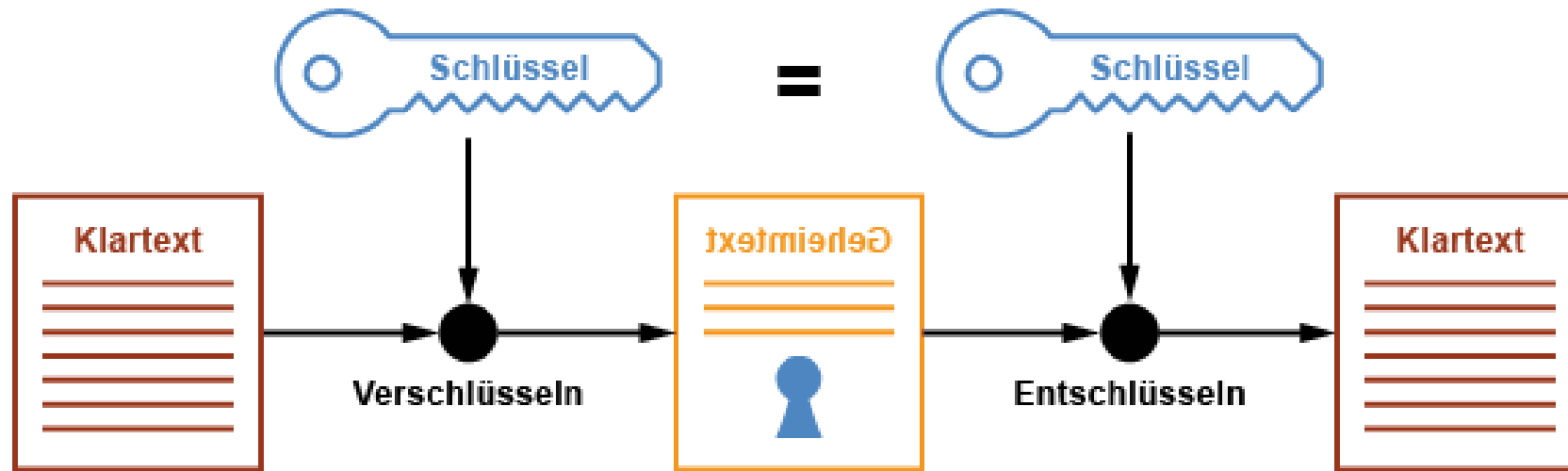


Verschlüsselung

Verschlüsselung



Symmetrisch



Symmetrisch (Secret-Key-Verfahren)

arbeitet mit einem einzigen Schlüssel

Schlüssel wird benutzt für

- Verschlüsselung
- Entschlüsselung

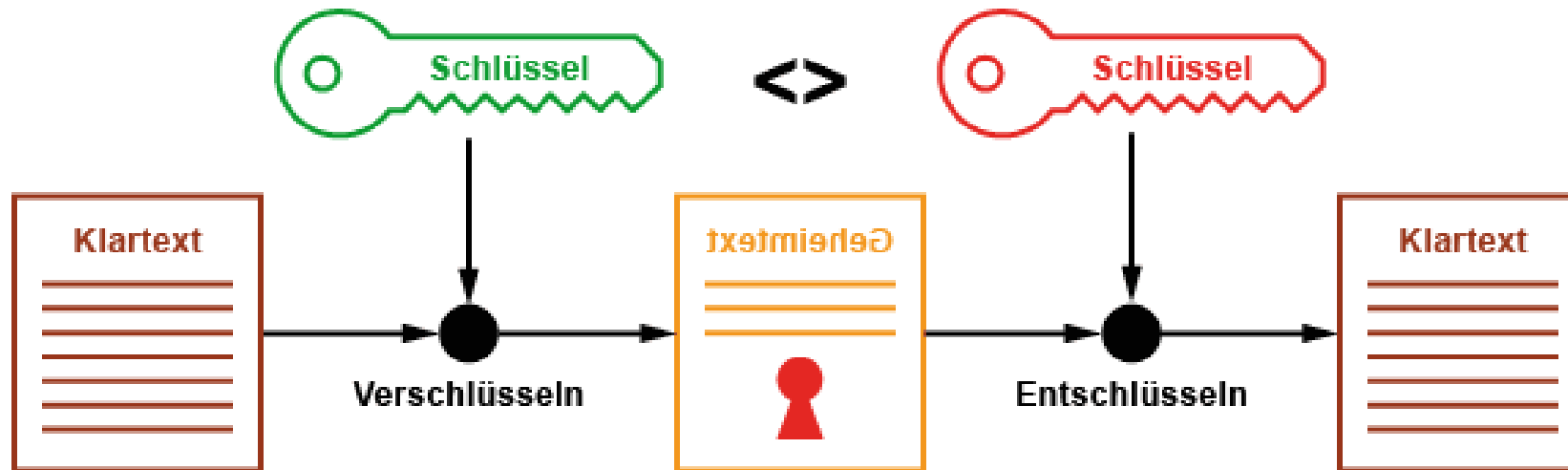
Verfahren ist schnell

bietet bei langen Schlüsseln Sicherheit

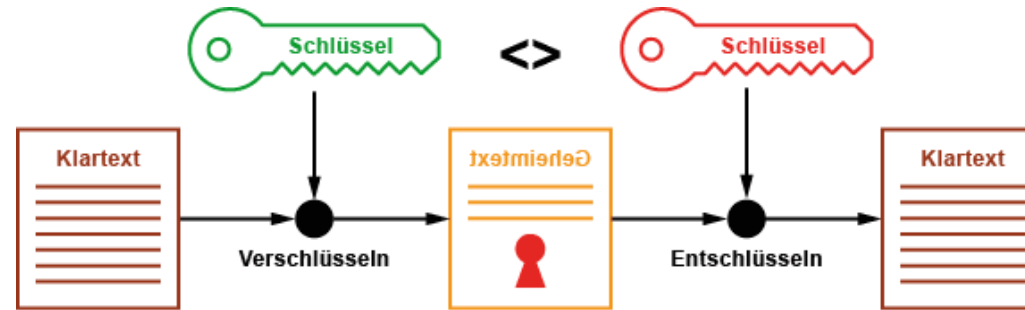
Problem: Schlüsselübergabe



Asymmetrisch



Asymmetrisch (Public-Key-Verschlüsselung)



Arbeitet mit Schlüsselpaaren

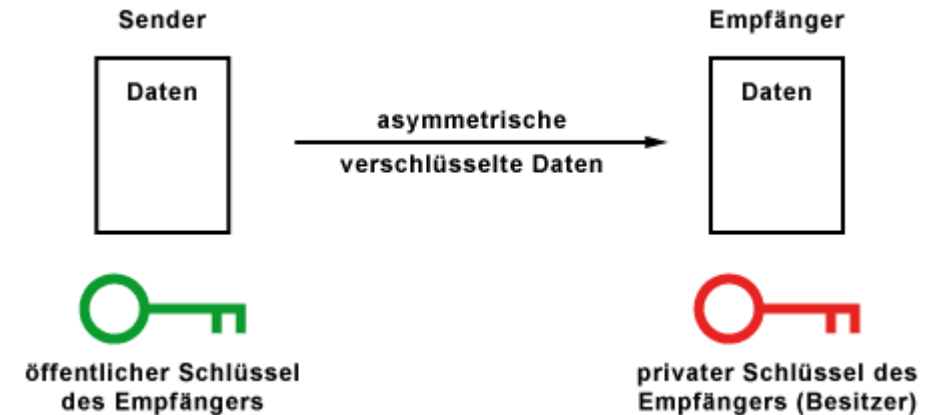
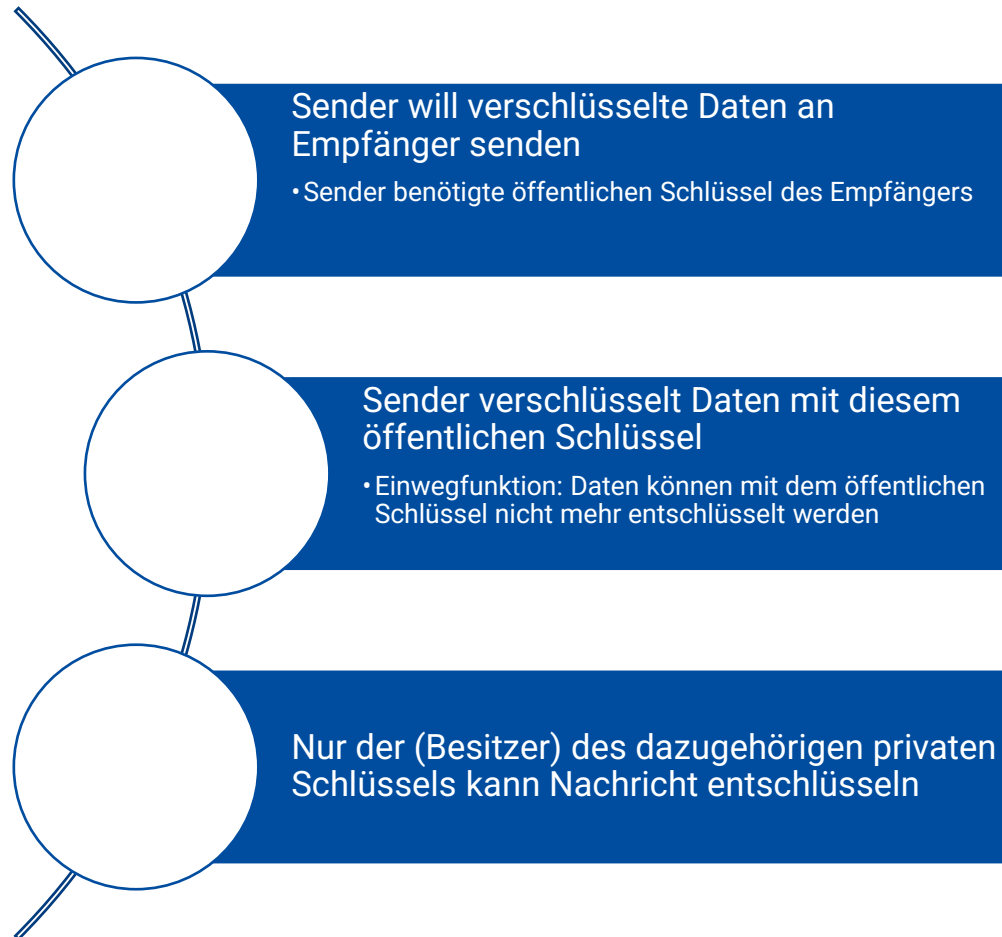
- public key (öffentlicher Schlüssel)
- private key (privater Schlüssel)
- hängen über mathematischen Algorithmus miteinander zusammen

Daten, die mit dem öffentlichen Schlüssel verschlüsselt werden, können nur mit dem privaten Schlüssel entschlüsselt werden


- private key muss unbedingt geheim gehalten werden

Asymmetrisch (Public-Key-Verschlüsselung)

Prinzip

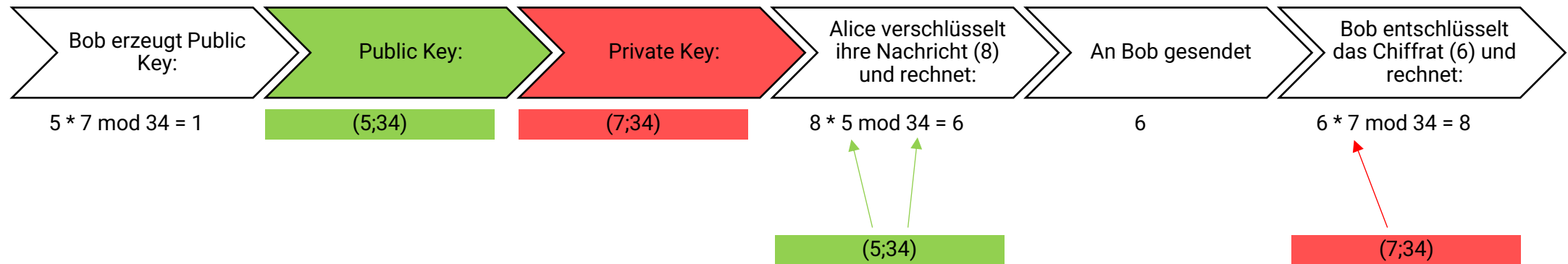


Primfaktorzerlegung



35	$= 5 \times 7$
77	$= 7 \times 11$
3233	$= 61 \times 53$

Ablauf Nachricht von Alice → Bob



Verbindung etablieren

