- Verfahren um Schlüssel zur Ver/Entschlüsselung über unsicheren Kanal zu versenden
- Verfahren
 - $-k, p \in \mathbb{N}$
 - Alice wählt geheime Zahl $a \in \mathbb{N}$ mit a < p

$$*A = k^a \bmod p$$

– Bob wählt geheime Zahl $b \in \mathbb{N}$ mit b < p

$$*B = k^b \bmod p$$

- A und B sind öffentlich
 - * public key
- Alice berechnet mithilfe von public key
 - $* B^a \mod p$
- Bob berechnet mithilfe von public key

$$* \ A^b \bmod \mathsf{p}$$

$$-B^a = k^{ab} = A^b$$

* Alice und Bob haben selben Schlüssel

[[Kryptographie]]