- m,k mit ggT(m,k)=1, m=pq
  - öffentlich
  - p,q sind unterschiedliche Primzahlen
  - N ursprüngliche Nachricht
  - N' verschlüsselte Nachricht
- Alice's Verschlüsselungsfunktion

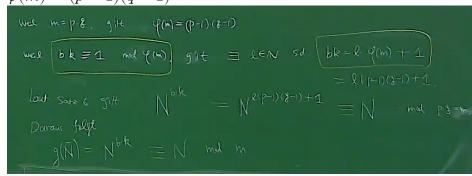
$$-\ f:1,...,m-1 -\!\!> \!\!1,...,m-1$$

- $x \rightarrow x^k \mod m$
- Bob wählt geheime Zahl b mit bk  $\equiv 1 \mod \varphi(m)$
- Bob's Entschlüsselfunktion:

$$-g:1,...,m-1->1,...,m-1$$

- $x \rightarrow x^b \mod m$
- [[Satz von Euler-Fermat]]

– 
$$\varphi(m)=(p-1)(q-1)$$



[[Kryptographie]]