

- $m, k \in \mathbb{N}$ mit $\text{ggT}(m, k) = 1$, $m = pq$
 - öffentlich
 - p, q sind unterschiedliche Primzahlen
 - N ursprüngliche Nachricht
 - N' verschlüsselte Nachricht
- Alice's Verschlüsselungsfunktion
 - $f : 1, \dots, m-1 \rightarrow 1, \dots, m-1$
 - $x \mapsto x^k \bmod m$
- Bob wählt geheime Zahl $b \in \mathbb{N}$ mit $bk \equiv 1 \bmod \varphi(m)$
- Bob's Entschlüsselungsfunktion:
 - $g : 1, \dots, m-1 \rightarrow 1, \dots, m-1$
 - $x \mapsto x^b \bmod m$
- [[Satz von Euler-Fermat]]
 - $\varphi(m) = (p-1)(q-1)$

Weil $m = p \cdot q$, gilt $\varphi(m) = (p-1)(q-1)$
 weil $bk \equiv 1 \bmod \varphi(m)$, gilt $\exists l \in \mathbb{N}$ sd. $bk = l \cdot \varphi(m) + 1$
 $\quad \quad \quad = l \cdot (p-1)(q-1) + 1$
 Laut Satz 6 gilt $N^{bk} = N^{l(p-1)(q-1)+1} \equiv N \bmod pq = m$
 Daraus folgt
 $g(N) = N^{bk} \equiv N \bmod m$

[[Kryptographie]]