RSA

1. Schlüssel anlegen
   Bob wählt zwei große Primzahlen p und q.
   Berechnet n:=p·q
   Wähle eine von $\phi(n)$ teilerfremde Zahl d.($\phi(n) = (p-1) \cdot (q-1)$)
   $\Rightarrow$ Es gibt ein Inverses i von d in $|\mathbb{Z}_n^*|$
   $d \cdot i \equiv 1(mod\ \phi(n))$
   Anmerkung: i kann mit dem erweiterten euklidischen Algorithmus errechnet werden.
   n,i werden öffentlich bekannt gegeben.

2. Alice: $m \in$
   $mathbbZ_n$ Nachricht
   c:=$m^i\ mod\ n$ (Al Kaschi)
   c wird an Bob geschickt.

3. Entschlüsseln: Bob berechnet $c^d\ mod\ n$
   Behauptung: $m \equiv c^d$ (mod n)
   $c^d = (m^i)^d = m^{i \cdot d} \equiv m^{1+n \cdot \phi(n)}$ mod n
   $id \equiv 1\ mod\ \phi(n)$, $m^{\phi(n)} \equiv 1$ (mod n)