Beschlennigung. RSA - Entschlüsselung  $n = p \cdot q$ ,  $q(n) = (p - n) \cdot (q - 1)$ Schlüssel: N.E., PIq, d öff. geheim m'= me mod n als verschlijsselte Nachricht Benechnung min moden mod P mod q mal mode-1 mod p, ebenso mod q vorher zeit O(logn) jetet O(log p + log q) Bitlänge von p,q. p·q=n, log p≈log q ≥ tog n  $\left(\frac{l_{0,1}n}{2}\right)^{3} + \left(\frac{l_{0,1}n}{2}\right)^{3} = \frac{1}{4} \log n$