RSA kryptering

Alice vil sende besked M til Bob, $M \in \mathbb{N}$.

Bob vælger primtal p og q og $e > 0$ så

$$\gcd((p-1)(q-1), e) = 1$$

(e som i encryption).

Bob finder $d > 0$ så $de \equiv 1 \pmod{(p-1)(q-1)}$.
D.v.s. d er invers til e modulo $(p-1)(q-1)$.
Hvis $\gcd((p-1)(q-1), e) = 1 = \lambda e + \mu(p-1)(q-1)$ så vælges d som det mindste positive tal der opfylder $d \equiv \lambda \pmod{(p-1)(q-1)}$.
(d som i decryption)

Bob sender $N = pq$ og e til Alice.

Vi antager $0 \leq M < N$ ellers deles beskeden i mindre dele.

Alice udregner $C = M^e \mod N$ ved "modular exponentiation" og sender C til Bob.

Bob udregner $C^d \mod N$ da dette tal er lig med M.

Bob bruger også modular exponentiation, men kan eventuelt udregne

$$C^d \mod p \quad \text{og} \quad C^d \mod q,$$

og bruge den kinesiske restsætning.