RSA Verschlüsselung

1. Wähle zwei große Primzahlen (mind. 100 Dezimalstellen) p und q; $n := pq$.
2. Wähle eine kleine natürliche Zahl e, die relativ prim zu $\varphi(n) = (p-1)(q-1)$ ist, und bestimme ein d mit $ed \equiv 1 \bmod \varphi(n)$.
3. *Öffentlicher Schlüssel:* $P = (e, n)$
4. *Privater Schlüssel:* $S = (d, n)$.

Verschlüsselung: $P(M) := M^e \bmod n$

Entschlüsselung: $S(C) := C^d \bmod n$.