RSA

Bob: public key n, e & private key p, q, d

s.t. $n = pq$ p, q prime

$\gcd(e, \underbrace{(p-1)(q-1)}_{\phi(n)}) = 1$

$de \equiv 1 \pmod{\phi(n)}$ ← this is necessary so d exists

choose p, q
compute n
choose e
compute d

Alice has a message $m < n$, $\gcd(m, n) = 1$

---

① Alice computes ciphertext:

$$c = m^e \pmod{n}$$

② Bob can decrypt:

$$m = c^d \pmod{n}$$

(Proof it works:

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m \pmod{n}$$
)