RSA Example

Computation

- $p = 17, q = 11, n = 187, e = 7$
- $\gcd(\phi(n), e) = 1, 1 < e < \phi(n)$
- $\gcd(160, 7) = 1$
- $d * 7 \equiv 1 \ (\mod 160)$
- **Solving:** $(d * 7) \mod 160 = 1 \implies d = 23$

Results

- PR = {d, n} = {23, 187}
- PU = {e, n} = {7, 187}

Test

- $M = 2$
- $C = M^e \mod n = 2^7 \mod 187 = 128$
- $M = C^d \mod n = 128^{23} \mod 187 = 2$