RSA Encryption (of numbers)

1. Choose 2 prime numbers p, q (30 digits each).
   p, q: secret
2. Multiply: $n = pq$
   n: public
3. Compute the totient: $\lambda(n) = LCM(p-1, q-1)$
   $\lambda(n)$: secret; LCM: least common multiple
4. Choose an encryption key: e (4 or more digits is good)
   e: public
   NEED: $GCD(e, \lambda) = 1$
5. Compute your decryption key: d = mod. inverse of e $(\text{mod } n)$
   d: secret
   ↳ $de \equiv 1 \pmod n$

ENCRYPT: Let m be a "message" (that is, a number between 0 and n)

Compute: $c = m^e \pmod n$

"cypher" encrypted message

(e, n) is the public key of the intended recipient

Post c for your recipient to see.

DECRYPT: compute $c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^1 = m \pmod n$

d: private key of the recipient

TEXT TO NUMBERS AND BACK